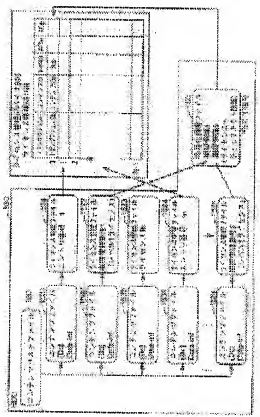
DATA TERMINAL DEVICE

Publication number: JP2002164881 (A)
Publication date: 2002-06-07
Inventor(s): HORI YOSHIHIRO; KAMIMURA TORU; HATAKEYAMA TAKAHISA; TAKAHASHI MASATAKA; TSUNEHIRO TAKASHI; OMORI YOSHIO
Applicant(s): SANYO ELECTRIC CO; FUJITSU LTD; PFU LTD; HITACHI LTD; NIPPON COLUMBIA
Classification:
- international: ***G06F13/00; G06F12/14; G06F21/24; G09C1/00; G10K15/02; H04L9/08; H04L9/32;*** **G06F13/00; G06F12/14; G06F21/00; G09C1/00; G10K15/02; H04L9/08; H04L9/32;** (IPC1-7): H04L9/08; G06F13/00; G09C1/00; H04L9/32
- European:
Application number: JP20000362913 20001129
Priority number(s): JP20000362913 20001129

Abstract of **JP 2002164881 (A)**
PROBLEM TO BE SOLVED: To provide a data terminal device, which can move encrypted contents data and license distributed by software to other data terminal devices. SOLUTION: A hard disc 530 in a personal computer has a contents list file 150 and an encrypted confidential file 160. A license management device 520 stores a binding key Kb into a license area 5215B of memory. The encrypted confidential file 160 can be decoded and encrypted by the binding key Kb stored in the license management device 520. The acquired license for the encrypted content data is stored in the encrypted confidential file 160 as confidential information.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－164881
（P2002－164881A）
(43)公開日　平成14年６月７日(2002.6.7)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｈ０４Ｌ　9/08		Ｇ０６Ｆ　13/00	５４０Ｓ	５Ｊ１０４
Ｇ０６Ｆ　13/00	５４０	Ｇ０９Ｃ　1/00	６６０Ａ	
Ｇ０９Ｃ　1/00	６６０		６６０Ｄ	
		Ｈ０４Ｌ　9/00	６０１Ｂ	
Ｈ０４Ｌ　9/32			６０１Ａ	

審査請求　未請求　請求項の数27　ＯＬ　（全109頁）　最終頁に続く

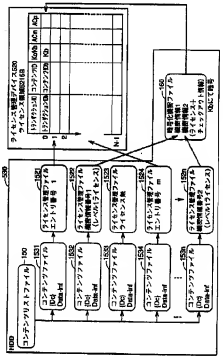
(21)出願番号　特願2000－362913(P2000－362913)

(22)出願日　平成12年11月29日(2000.11.29)

(71)出願人　000001889
三洋電機株式会社
大阪府守口市京阪本通２丁目５番５号
(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(71)出願人　000136136
株式会社ピーエフユー
石川県河北郡宇ノ気町字宇野気ヌ98番地の２
(74)代理人　100064746
弁理士　深見　久郎　（外３名）
最終頁に続く

(54)【発明の名称】　データ端末装置

(57)【要約】
【課題】　ソフトウエアによって配信された暗号化コンテンツデータおよびライセンスを他のデータ端末装置へ移動可能なデータ端末装置を提供する。
【解決手段】　パーソナルコンピュータのハードディスク５３０は、コンテンツリストファイル１５０と暗号化機密ファイル１６０とを有する。ライセンス管理デバイス５２０は、メモリのライセンス領域５２１５Ｂにバインディング鍵Ｋｂを格納する。暗号化機密ファイル１６０は、ライセンス管理デバイス５２０に格納されたバインディング鍵Ｋｂによって復号および暗号化が可能である。そして、取得された暗号化コンテンツデータのライセンスは、暗号化機密ファイル１６０に機密情報として格納される。



1

【特許請求の範囲】

【請求項１】　コンテンツデータを暗号化した暗号化コンテンツデータおよび前記暗号化コンテンツデータを復号して元の平文を得るためのライセンスを取得し、前記暗号化コンテンツデータおよび前記ライセンスを他のデータ端末装置へ出力するデータ端末装置であって、

前記暗号化コンテンツデータおよび前記ライセンスをソフトウエアによって取得するモジュール部と、

前記暗号化コンテンツデータと、ライセンス管理ファイルと、暗号化機密ファイルとを記憶する記憶部と、

前記暗号化機密ファイルを復号し、かつ、その復号した機密ファイルを暗号化するバインディング鍵を含むバインディングライセンスを専用領域に格納するデバイス部とを備え、

前記機密ファイルは、前記ライセンスを構成要素とする機密情報を含み、

前記ライセンス管理ファイルは、前記暗号化コンテンツファイルに対応し、かつ、前記機密ファイルに含まれる前記機密情報の管理番号を含む、データ端末装置。

【請求項２】　前記暗号化機密ファイルの初期化時、

前記モジュール部は、前記バインディング鍵を含めて前記バインディングライセンスを生成し、機密情報が空な機密ファイルを生成し、その生成した機密ファイルを前記生成したバインディング鍵によって暗号化して前記暗号化機密ファイルを生成するとともに、前記生成したバインディングライセンスを前記デバイス部に与える、請求項１に記載のデータ端末装置。

【請求項３】　前記ライセンスの取得時、

前記モジュール部は、前記記憶部から読出した前記暗号化機密ファイルを前記デバイス部から取得した前記バインディング鍵によって復号し、その復号した機密ファイルに前記取得したライセンスを機密情報として書込んで前記機密ファイルを更新し、その更新した機密ファイルを前記バインディング鍵によって暗号化し、その暗号化した暗号化機密ファイルを前記記憶部に更新記録し、前記書込んだライセンスを構成要素とする機密情報の管理番号を含むライセンス管理ファイルを作成して前記記憶部に書込む、請求項１に記載のデータ端末装置。

【請求項４】　前記ライセンスの送信時、

前記モジュール部は、前記デバイス部から取得した前記バインディング鍵によって前記記憶部から読出した前記暗号化機密ファイルを復号してライセンスを取得し、その取得したライセンスを外部へ出力する、請求項１に記載のデータ端末装置。

【請求項５】　前記ライセンスの出力時、

前記モジュール部は、前記ライセンスに対応し、かつ前記記憶部に記録された前記暗号化コンテンツデータと前記ライセンスとを外部へ出力する、請求項４に記載のデータ端末装置。

【請求項６】　前記デバイス部は、前記専用領域を指定する専用登録番号を前記モジュール部から受取り、その受取った専用登録番号によって前記バインディングライセンスを前記専用領域に格納する、請求項１に記載のデータ端末装置。

2

【請求項７】　前記ライセンスの出力時、

前記モジュール部は、前記専用登録番号を前記デバイス部へ送信することによって前記バインディング鍵を取得する、請求項６に記載のデータ端末装置。

【請求項８】　前記ライセンスの出力時、

前記モジュール部は、前記デバイス部に対する認証データを前記デバイス部へ送信し、前記デバイス部において前記認証データが認証された場合、前記バインディング鍵を取得する、請求項１から請求項７のいずれか１項に記載のデータ端末装置。

【請求項９】　前記ライセンスの出力時、

前記デバイス部は、前記バインディング鍵を暗号化して出力する、請求項１から請求項８のいずれか１項に記載のデータ端末装置。

【請求項１０】　前記ライセンスの出力時、

前記モジュール部は、前記取得したバインディング鍵によって前記暗号化機密ファイルを復号して機密ファイルを取得し、かつ、前記記憶部から読出したライセンス管理ファイルに含まれる機密情報の管理番号に一致する機密情報を前記取得した機密ファイルから読出すことによって外部へ出力するライセンスを取得する、請求項４に記載のデータ端末装置。

【請求項１１】　前記ライセンスの他のデータ端末装置への送信時、

前記モジュール部は、さらに、前記デバイス部において保持された公開暗号鍵を受取ることによって前記デバイス部はバインディングライセンスの書込みが可能であることを確認する、請求項１から請求項９のいずれか１項に記載のデータ端末装置。

【請求項１２】　前記暗号化コンテンツデータの他のデータ端末装置への移動時、

前記モジュール部は、前記ライセンスの複製ができないとき、前記他のデータ端末装置へ送信したライセンスを構成要素とする機密情報を削除し、その削除した機密情報の管理番号を削除してライセンス管理ファイルを更新し、もう１つのバインディング鍵を生成し、その生成したもう１つのバインディング鍵によって機密ファイルを暗号化して前記暗号化機密ファイルを更新する、請求項１０に記載のデータ端末装置。

【請求項１３】　前記暗号化コンテンツデータの他のデータ端末装置への移動時、

前記デバイス部は、前記もう１つのバインディング鍵を含むもう１つのバインディングライセンスを前記モジュール部から受け取り、その受取ったもう１つのバインディングライセンスを前記専用領域に上書きして格納する、請求項１１に記載のデータ端末装置。

【請求項１４】　前記ライセンスの他のデータ端末装置への送信時、
前記モジュール部は、前記他のデータ端末装置から受信した認証データを認証すると、ライセンスを他のデータ端末装置へ送信する、請求項１から請求項１２のいずれか１項に記載のデータ端末装置。
【請求項１５】　前記モジュール部は、前記ライセンスを暗号化した上で出力する、請求項１３に記載のデータ端末装置。
【請求項１６】　コンテンツデータを暗号化した暗号化コンテンツデータおよび前記暗号化コンテンツデータを復号して元の平文を得るためのライセンスを取得し、前記暗号化コンテンツデータおよび前記ライセンスを他のデータ端末装置へ出力するデータ端末装置であって、
前記暗号化コンテンツデータおよび前記ライセンスをソフトウエアによって取得するモジュール部と、
前記暗号化コンテンツデータと、ライセンス管理ファイルと、独自の暗号化を施した暗号化機密ファイルとを記憶する記憶部と、
バインディング鍵を含むバインディングライセンスを専用領域に格納するデバイス部とを備え、
前記暗号化機密ファイルを復号した機密ファイルは、前記デバイス部が格納するバインディングライセンスと同じバインディングライセンスを含み、
前記ライセンス管理ファイルは、前記暗号化コンテンツデータに対応し、かつ、前記ライセンスを構成要素とする機密情報に独自の暗号化を施した暗号化機密情報を含む、データ端末装置。
【請求項１７】　前記暗号化機密ファイルの初期化時、
前記モジュール部は、前記バインディング鍵を含めて前記バインディングライセンスを生成し、その生成したバインディングライセンスを格納した機密ファイルを生成し、その生成した機密ファイルに独自の暗号化を施して前記暗号化機密ファイルを生成するとともに、前記生成したバインディングライセンスを前記デバイス部に与える、請求項１６に記載のデータ端末装置。
【請求項１８】　前記ライセンスの取得時、
前記モジュール部は、前記ライセンスに独自の暗号化を施して暗号化機密情報を生成し、その暗号化機密情報を含むライセンス管理ファイルを生成して前記記憶部に書込む、請求項１６に記載のデータ端末装置。
【請求項１９】　前記ライセンスの送信時、
前記モジュール部は、前記デバイス部から取得した前記バインディング鍵が前記暗号化機密ファイルを復号して取得したバインディング鍵に一致すると、前記記憶部から読出した前記暗号化機密情報を復号してライセンスを取得し、その取得したライセンスと前記記憶部から読出した暗号化コンテンツデータとを他のデータ端末装置へ送信する、請求項１８に記載のデータ端末装置。
【請求項２０】　前記独自の暗号化方式は、データ端末装置から取得可能なデータ端末装置に固有の情報に関連付けた暗号化方式である、請求項１６に記載のデータ端末装置。
【請求項２１】　前記デバイス部は、前記専用領域を指定する専用登録番号を前記モジュール部から受取り、その受取った専用登録番号によって前記バインディングライセンスを前記専用領域に格納し、
前記モジュール部は、前記専用登録番号を含めて前記暗号化機密ファイルおよび前記ライセンス管理ファイルを生成する、請求項１６に記載のデータ端末装置。
【請求項２２】　前記ライセンスの送信時、
前記モジュール部は、前記専用登録番号を前記デバイス部へ送信することによって前記バインディング鍵を取得する、請求項２１に記載のデータ端末装置。
【請求項２３】　前記ライセンスの他のデータ端末装置への送信時、
前記モジュール部は、前記デバイス部に対する認証データを前記デバイス部へ送信し、前記デバイス部において前記認証データが認証された場合、前記バインディング鍵を取得する、請求項１６から請求項２３のいずれか１項に記載のデータ端末装置。
【請求項２４】　前記ライセンスの他のデータ端末装置への送信時、
前記モジュール部は、前記他のデータ端末装置から受信した認証データを認証すると、ライセンスを他のデータ端末装置へ送信する、請求項１６から請求項２３のいずれか１項に記載のデータ端末装置。
【請求項２５】　前記モジュール部は、配信サーバからインターネットによって前記暗号化コンテンツデータおよび前記ライセンスを取得する、請求項１から請求項２４のいずれか１項に記載のデータ端末装置。
【請求項２６】　記録媒体から平文のコンテンツデータを読出す媒体駆動部をさらに備え、
前記モジュール部は、前記媒体駆動部が読出したコンテンツデータに含まれる複製可否情報に基づいてライセンスを生成し、その生成したライセンスに含まれるライセンス鍵によって前記コンテンツデータを暗号化して暗号化コンテンツデータを生成することによって前記暗号化コンテンツデータおよび前記ライセンスを取得する、請求項１から請求項２４のいずれか１項に記載のデータ端末装置。
【請求項２７】　前記デバイス部は、さらに、配信サーバから前記暗号化コンテンツデータおよびライセンスを受信し、その受信したライセンスを保持し、
前記記憶部は、前記デバイス部によって受信された暗号化コンテンツデータを記憶する、請求項１から請求項２４のいずれか１項に記載のデータ端末装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、コピーされた情

5

報に対する著作権保護を可能とするデータ配信システムにおいて用いられるデータ端末装置に関するものである。

【０００２】【従来の技術】近年、インターネット等の情報通信網等の進歩により、再生端末等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【０００３】このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【０００４】したがって、このような情報通信網上において音楽データや画像データ等の著作者の権利が存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【０００５】一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【０００６】ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したＣＤ（コンパクトディスク）については、ＣＤから光磁気ディスク（ＭＤ等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やＭＤ等の媒体の代金のうちの一定額を間接的に著作権者に対して著作権料として支払うことになっている。

【０００７】しかも、ＣＤからＭＤへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なＭＤからさらに他のＭＤに音楽データとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【０００８】このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権侵害のための十分な方策が講じられる必要がある。

【０００９】この場合、情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されること、あるいは、複製でき

6

ても利用されることを防止することが必要となる。

【００１０】そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、再生端末等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を送信する。そして、暗号化コンテンツデータやライセンス鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【００１１】最後的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンスと、暗号化コンテンツデータをメモリカードに送信する。そして、メモリカードは、受信したライセンスと暗号化コンテンツデータをメモリカードに記録する。

【００１２】そして、メモリカードに記録した暗号化コンテンツデータを再生するときは、メモリカードを携帯電話機に装着する。携帯電話機は、通常の電話機能の他にメモリカードからの暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。

【００１３】このように、携帯電話機のユーザは、携帯電話機を用いて暗号化コンテンツデータを配信サーバから受信し、その暗号化コンテンツデータを再生することができる。

【００１４】一方、インターネットを用いて暗号化コンテンツデータをパーソナルコンピュータに配信することも行なわれている。そして、パーソナルコンピュータへの暗号化コンテンツデータとライセンスを同様な方法で配信することは可能ではあるが、パーソナルコンピュータにインストールされたソフトウェアによって暗号化コンテンツデータおよびライセンスの配信が受信され、ライセンスの保護が行なわれており、受信した暗号化コンテンツデータおよびライセンスを他のパーソナルコンピュータへ移動することは著作権保護の観点から行なわれていない。

【００１５】つまり、パーソナルコンピュータへ配信されたライセンスを記録したパーソナルコンピュータのＣＰＵに個別に付与された識別番号や起動プログラムであるＢＩＯＳの識別番号などの値に関連付けた暗号処理を用いて、そのまま他のパーソナルコンピュータにコピーしても、ライセンスを取り出せず、暗号化コンテンツ復

号して再生できない管理構造を採用している。そして、この管理下においてライセンスを他のパーソナルコンピュータへ移動できるサービスを提供したとすると、記録装置上で、ライセンスを特定することはできないものの、暗号化コンテンツデータおよびライセンスを管理し、記録している全てのデータのバックアップを取っておき、提供されたサービスによって、他のパーソナルコンピュータへ暗号化コンテンツデータおよびライセンスを移動させた後に、バックアップを取った暗号化コンテンツデータおよびライセンスを管理し、記録している全てのデータをパーソナルコンピュータへ戻せば移動前の状態を再現でき、暗号化コンテンツデータおよびライセンスを複製したのと同じことになる。このような管理においてのライセンスの移動は、セキュリティホールが明らかに存在する。したがって、ソフトウエアによってパーソナルコンピュータへ配信された暗号化コンテンツデータおよびライセンスを他のパーソナルコンピュータへ移動できないことになっている。

【００１６】

【発明が解決しようとする課題】しかし、パーソナルコンピュータに配信された暗号化コンテンツデータおよびライセンスをそのパーソナルコンピュータから、一切、取り出すことができないとすると、パーソナルコンピュータの破損や、バージョンアップによってＣＰＵが変動したときは、既に受信した暗号化コンテンツデータおよびライセンスを利用することができないという問題がある。

【００１７】そこで、本発明は、かかる問題を解決するためになされたものであり、その目的は、ソフトウエアによって配信された暗号化コンテンツデータおよびライセンスを他のデータ端末装置へ移動可能なデータ端末装置を提供することである。

【００１８】

【課題を解決するための手段および発明の効果】この発明によるデータ端末装置は、コンテンツデータを暗号化した暗号化コンテンツデータおよび暗号化コンテンツデータを復号して元の平文を得るためのライセンスを取得し、暗号化コンテンツデータおよびライセンスを他のデータ端末装置へ出力するデータ端末装置であって、暗号化コンテンツデータおよびライセンスをソフトウエアによって取得するモジュール部と、暗号化コンテンツデータと、ライセンス管理ファイルと、暗号化機密ファイルとを記憶する記憶部と、暗号化機密ファイルを復号し、かつ、その復号した機密ファイルを暗号化するバインディング鍵を含むバインディングライセンスを専用領域に格納するデバイス部とを備え、機密ファイルは、ライセンスを構成要素とする機密情報を含み、ライセンス管理ファイルは、暗号化コンテンツファイルに対応し、かつ、機密ファイルに含まれる機密情報の管理番号を含む。

【００１９】この発明によるデータ端末装置においては、モジュール部は、ソフトウェアによって暗号化コンテンツデータおよびライセンスを取得し、デバイス部から取出したバインディング鍵によって暗号化機密ファイルを復号し、取得したライセンスを復号した機密ファイルに書込み、バインディング鍵によって機密ファイルを暗号化して暗号化機密ファイルを生成する。つまり、モジュール部は、デバイス部においてハードウェアによって保持されるバインディング鍵を介して暗号化機密ファイルを開閉して取得したライセンスを管理する。

【００２０】したがって、この発明によれば、ソフトウェアによって取得された暗号化コンテンツデータを復号して再生するためのライセンスは、ハードウェアに保持されたバインディング鍵によって管理されるため、取得した暗号化コンテンツデータおよびライセンスを他のデータ端末装置へ移動できる。

【００２１】好ましくは、暗号化機密ファイルの初期化時、データ端末装置のモジュール部は、バインディング鍵を含めてバインディングライセンスを生成し、機密情報が空な機密ファイルを生成し、その生成した機密ファイルを生成したバインディング鍵によって暗号化して暗号化機密ファイルを生成するとともに、生成したバインディングライセンスをデバイス部に与える。

【００２２】暗号化機密ファイルの初期化時、モジュール部は、バインディング鍵を含むバインディングライセンスと空な機密ファイルとを生成し、機密ファイルをバインディング鍵によって暗号化を行なって暗号化機密ファイルを生成するとともにバインディングライセンスをデバイス部に保持する。

【００２３】したがって、この発明によれば、ソフトウェアによって取得した暗号化コンテンツデータのライセンスを格納する機密ファイルをソフト的に作成し、その作成した機密ファイルを管理するためのバインディングライセンスをハード的に管理できる。

【００２４】好ましくは、ライセンスの取得時、データ端末装置のモジュール部は、記憶部から読出した暗号化機密ファイルをデバイス部から取得したバインディング鍵によって復号し、その復号した機密ファイルに取得したライセンスを機密情報として書込んで機密ファイルを更新し、その更新した機密ファイルをバインディング鍵によって暗号化し、その暗号化した暗号化機密ファイルを記憶部に更新記録し、書込んだライセンスを構成要素とする機密情報の管理番号を含むライセンス管理ファイルを作成して記憶部に書込む。

【００２５】デバイス部から取得したバインディング鍵によって暗号化機密ファイルを開閉して取得したライセンスを機密ファイルに書込む。そして、その書込んだライセンスを構成要素とする機密情報の管理番号を含めてライセンス管理ファイルを作成する。

【００２６】したがって、この発明によれば、ソフト的

に取得した暗号化コンテンツデータのライセンスを管理番号によって管理できる。

【００２７】好ましくは、ライセンスの送信時、データ端末装置のモジュール部は、デバイス部から取得したバインディング鍵によって記憶部から読出した暗号化機密ファイルを復号してライセンスを取得し、その取得したライセンスを外部へ出力する。

【００２８】モジュール部は、デバイス部から取得したバインディング鍵によって暗号化機密ファイルを復号してライセンスを取得し、その取得したライセンスを外部へ出力する。

【００２９】したがって、この発明によれば、ソフト的に取得した暗号化コンテンツデータのライセンスをハード的に取得した暗号化コンテンツデータのライセンスと同じように他の装置へ移動できる。

【００３０】好ましくは、データ端末装置のモジュール部は、ライセンスの出力時、ライセンスに対応し、かつ記憶部に記録された暗号化コンテンツデータとライセンスとを外部へ出力する。

【００３１】ライセンスの外部への出力時、機密ファイルから取出したライセンスに対応する暗号化コンテンツデータを記憶部から読出し、暗号化コンテンツデータとライセンスとを外部へ出力する。

【００３２】したがって、この発明によれば、暗号化コンテンツデータおよびライセンスをソフト的に読出して他の装置へ暗号化コンテンツデータおよびライセンスを移動できる。

【００３３】好ましくは、データ端末装置のデバイス部は、専用領域を指定する専用登録番号をモジュール部から受取り、その受取った専用登録番号によってバインディングライセンスを専用領域に格納する。

【００３４】デバイス部は、専用登録番号を介して暗号化機密ファイルを開閉するためのバインディングライセンスを専用領域に格納する。

【００３５】したがって、この発明によれば、専用登録番号によってバインディングライセンスと暗号化コンテンツデータのライセンスとを対応付けることができる。

【００３６】好ましくは、ライセンスの出力時、データ端末装置のモジュール部は、専用登録番号をデバイス部へ送信することによってバインディング鍵を取得する。

【００３７】モジュール部は、専用登録番号を介して、記憶部から読出したいライセンスが格納された機密ファイルを開けるためのバインディング鍵を取得する。

【００３８】したがって、この発明によれば、専用登録番号によってバインディング鍵を正確に取得できる。

【００３９】好ましくは、ライセンスの出力時、データ端末装置のモジュール部は、デバイス部に対する認証データをデバイス部へ送信し、デバイス部において認証データが認証された場合、バインディング鍵を取得する。

【００４０】認証されたモジュール部のみにバインディング鍵が与えられる。したがって、この発明によれば、不正なバインディング鍵の流出を防止できる。

【００４１】好ましくは、ライセンスの出力時、データ端末装置のデバイス部は、バインディング鍵を暗号化して出力する。

【００４２】デバイス部は、ライセンスを管理するためのバインディング鍵を暗号化して出力する。

【００４３】したがって、この発明によれば、ライセンスを他の装置へ移動するとき、移動先でライセンスを管理するバインディング鍵を不正に取得されにくくできる。

【００４４】好ましくは、ライセンスの出力時、データ端末装置のモジュール部は、取得したバインディング鍵によって暗号化機密ファイルを復号して機密ファイルを取得し、かつ、記憶部から読出したライセンス管理ファイルに含まれる機密情報の管理番号に一致する機密情報を取得した機密ファイルから読出すことによって外部へ出力するライセンスを取得する。

【００４５】モジュール部は、デバイス部からバインディング鍵を取得して暗号化機密ファイルを復号し、その復号した機密ファイルに含まれる機密情報から管理番号に一致する機密情報を取得して外部へ出力しようとするライセンスを取得する。

【００４６】したがって、この発明によれば、管理番号を介して正確にライセンスを取得できる。

【００４７】好ましくは、ライセンスの他のデータ端末装置への送信時、データ端末装置のモジュール部は、さらに、デバイス部において保持された公開暗号鍵を受取ることによってデバイス部はバインディングライセンスの書込みが可能であることを確認する。

【００４８】モジュール部は、ライセンスの他の装置への送信時、デバイス部がバインディングライセンスの書込みが可能なデバイス部か否かをデバイス部から公開暗号鍵を受取ることによって確認する。

【００４９】したがって、この発明によれば、暗号化コンテンツデータのライセンスを移動した際、デバイス部に格納されたバインディングライセンスを書換えることによってライセンスを移動したことを認識可能である。

【００５０】好ましくは、暗号化コンテンツデータの他のデータ端末装置への移動時、データ端末装置のモジュール部は、ライセンスの複製ができないとき、他のデータ端末装置へ送信したライセンスを構成要素とする機密情報を削除し、その削除した機密情報の管理番号を削除してライセンス管理ファイルを更新し、もう１つのバインディング鍵を生成し、その生成したもう１つのバインディング鍵によって機密ファイルを暗号化して暗号化機密ファイルを更新する。

【００５１】移動したライセンスの複製が禁止されているとき、モジュール部は、移動したライセンスを削除するとともに、別のバインディング鍵を生成して暗号化機

密ファイルを更新する。

【００５２】したがって、この発明によれば、ライセンスが不正に複製されるのを防止できる。

【００５３】好ましくは、暗号化コンテンツデータの他のデータ端末装置への移動時、データ端末装置のデバイス部は、もう１つのバインディング鍵を含むもう１つのバインディングライセンスをモジュール部から受け取り、その受取ったもう１つのバインディングライセンスを専用領域に上書きして格納する。

【００５４】別のバインディング鍵が生成されたとき、デバイス部においてバインディングライセンスの書換えが行なわれる。

【００５５】したがって、この発明によれば、最新のバインディングライセンスによって暗号化コンテンツデータを再生するためのライセンスを管理できる。

【００５６】好ましくは、ライセンスの他のデータ端末装置への送信時、データ端末装置のモジュール部は、他のデータ端末装置から受信した認証データを認証すると、ライセンスを他のデータ端末装置へ送信する。

【００５７】モジュール部は、暗号化コンテンツデータのライセンスを移動しようとするデータ端末装置が正規の端末装置であることを確認してから暗号化コンテンツデータのライセンスを送信する。

【００５８】したがって、この発明によれば、正規なデータ端末装置間で暗号化コンテンツデータのライセンスを移動でき、暗号化コンテンツデータを十分に保護できる。

【００５９】好ましくは、データ端末装置のモジュール部は、ライセンスを暗号化した上で出力する。

【００６０】モジュール部は、ライセンスを暗号化した上で他のデータ端末装置へ移動する。

【００６１】したがって、この発明によれば、ライセンスの移動時に、そのライセンスを不正に取得されにくい。

【００６２】また、この発明によるデータ端末装置は、コンテンツデータを暗号化した暗号化コンテンツデータおよび暗号化コンテンツデータを復号して元の平文を得るためのライセンスを取得し、暗号化コンテンツデータおよびライセンスを他のデータ端末装置へ出力するデータ端末装置であって、暗号化コンテンツデータおよびライセンスをソフトウエアによって取得するモジュール部と、暗号化コンテンツデータと、ライセンス管理ファイルと、独自の暗号化を施した暗号化機密ファイルとを記憶する記憶部と、バインディング鍵を含むバインディングライセンスを専用領域に格納するデバイス部とを備え、暗号化機密ファイルを復号した機密ファイルは、デバイス部が格納するバインディングライセンスと同じバインディングライセンスを含み、ライセンス管理ファイルは、暗号化コンテンツデータに対応し、かつ、ライセンスを構成要素とする機密情報に独自の暗号化を施した暗号化機密情報を含む。

【００６３】この発明によるデータ端末装置においては、モジュール部は、ソフトウエアによって暗号化コンテンツデータおよびライセンスを取得し、その取得したライセンスに独自の暗号化を施して暗号化機密情報を生成し、その生成した暗号化機密情報を含むライセンス管理ファイルを作成して記憶部に書込む。また、ライセンスを管理するバインディングライセンスは機密ファイルに格納される。

【００６４】したがって、この発明によれば、ライセンスを管理するためのバインディング鍵はハードウエアによって保持されるため、ソフトウエアによって取得された暗号化コンテンツデータを復号して再生するためのライセンスを他のデータ端末装置へ移動できる。

【００６５】好ましくは、暗号化機密ファイルの初期化時、データ端末装置のモジュール部は、バインディング鍵を含めてバインディングライセンスを生成し、その生成したバインディングライセンスを格納した機密ファイルを生成し、その生成した機密ファイルに独自の暗号化を施して暗号化機密ファイルを生成するとともに、生成したバインディングライセンスをデバイス部に与える。

【００６６】モジュール部は、暗号化機密ファイルの初期化時、バインディング鍵を含むバインディングライセンスと空な機密ファイルとを生成し、機密ファイルに生成したバインディングライセンスを書込んで独自の暗号化を行なって暗号化機密ファイルを生成するとともにバインディングライセンスをデバイス部の専用領域に保持する。

【００６７】したがって、この発明によれば、ライセンスを管理するためのバインディング鍵はハードウエアによって保持されるため、ソフトウエアによって取得された暗号化コンテンツデータを復号して再生するためのライセンスを他のデータ端末装置へ移動できる。

【００６８】好ましくは、ライセンスの取得時、データ端末装置のモジュール部は、ライセンスに独自の暗号化を施して暗号化機密情報を生成し、その暗号化機密情報を含むライセンス管理ファイルを生成して記憶部に書込む。

【００６９】モジュール部は、取得したライセンスに独自の暗号化を施して記憶部で管理する。

【００７０】したがって、この発明によれば、ライセンスを独自の暗号化方式によって管理できる。

【００７１】好ましくは、ライセンスの送信時、データ端末装置のモジュール部は、デバイス部から取得したバインディング鍵が暗号化機密ファイルを復号して取得したバインディング鍵に一致すると、記憶部から読出した暗号化機密情報を復号してライセンスを取得し、その取得したライセンスと記憶部から読出した暗号化コンテンツデータとを他のデータ端末装置へ送信する。

【００７２】モジュール部は、デバイス部に格納された

バインディング鍵と記憶部に格納されたバインディング鍵とが一致する場合に限り、ライセンスを取得する。

【００７３】したがって、ハード的に管理されたバインディング鍵と同じバインディング鍵を有するモジュール部だけがライセンスを取得できる。

【００７４】好ましくは、独自の暗号化方式は、データ端末装置から取得可能なデータ端末装置に固有の情報に関連付けた暗号化方式である。

【００７５】モジュール部は、データ端末装置に固有な情報、たとえば、ＣＰＵのバージョン番号等に基づいた暗号化方式によってライセンスを暗号化する。

【００７６】したがって、この発明によれば、暗号化されたライセンスが他の装置へ不正に流出されても、そのライセンスが不正に取得されない。

【００７７】好ましくは、データ端末装置のデバイス部は、専用領域を指定する専用登録番号をモジュール部から受取り、その受取った専用登録番号によってバインディングライセンスを専用領域に格納し、モジュール部は、専用登録番号を含めて暗号化機密ファイルおよびライセンス管理ファイルを生成する。

【００７８】デバイス部は、モジュール部によって生成された専用登録番号によってバインディングライセンスをハード的に管理し、モジュール部は、生成した専用登録番号と取得したライセンスとを独自に暗号化してソフト的に管理する。

【００７９】したがって、この発明によれば、モジュール部は、専用登録番号を介してデバイス部に保持されたバインディング鍵を取得し、暗号化機密ファイルから読出したバインディング鍵とデバイス部から取得したバインディング鍵との一致を正確に判別できる。

【００８０】好ましくは、ライセンスの送信時、データ端末装置のモジュール部は、専用登録番号をデバイス部へ送信することによってバインディング鍵を取得する。

【００８１】モジュール部は、専用登録番号をデバイス部へ送信し、デバイス部は受信した専用登録番号によって指定された専用領域からバインディング鍵を取出して出力する。

【００８２】したがって、この発明によれば、専用登録番号によってバインディング鍵を正確に取得できる。

【００８３】好ましくは、ライセンスの他のデータ端末装置への送信時、データ端末装置のモジュール部は、デバイス部に対する認証データをデバイス部へ送信し、デバイス部において認証データが認証された場合、バインディング鍵を取得する。

【００８４】モジュール部のデバイス部に対する正当性が確認された場合だけ、モジュール部がバインディング鍵を取得する。

【００８５】したがって、この発明によれば、バインディング鍵の不正な取得を防止でき、その結果、ライセンスが他の端末装置へ不正に移動されることを防止できる。

【００８６】好ましくは、ライセンスの他のデータ端末装置への送信時、データ端末装置のモジュール部は、他のデータ端末装置から受信した認証データを認証すると、ライセンスを他のデータ端末装置へ送信する。

【００８７】暗号化コンテンツデータおよびライセンスを移動しようとするデータ端末装置が正規であることが確認されると、モジュール部は暗号化コンテンツデータおよびライセンスを他のデータ端末装置へ送信する。

【００８８】したがって、この発明によれば、正規のデータ端末装置間でのみ、暗号化コンテンツデータおよびライセンスの移動が可能である。

【００８９】好ましくは、データ端末装置のモジュール部は、配信サーバからインターネットによって暗号化コンテンツデータおよびライセンスを取得する。

【００９０】したがって、この発明によれば、各種のコンテンツデータを取得し、かつ、他の端末装置へ取得したコンテンツデータを移動できる。

【００９１】好ましくは、データ端末装置は、記録媒体から平文のコンテンツデータを読出す媒体駆動部をさらに備え、モジュール部は、媒体駆動部が読出したコンテンツデータに含まれる複製可否情報に基づいてライセンスを生成し、その生成したライセンスに含まれるライセンス鍵によってコンテンツデータを暗号化して暗号化コンテンツデータを生成することによって暗号化コンテンツデータおよびライセンスを取得する。

【００９２】データ端末装置は、リッピングによって暗号化コンテンツデータおよびライセンスを取得する。

【００９３】したがって、この発明によれば、通信手段以外の手段で頒布されるコンテンツデータも取得し、他のデータ端末装置へ移動できる。

【００９４】好ましくは、データ端末装置のデバイス部は、さらに、配信サーバから暗号化コンテンツデータおよびライセンスを受信し、その受信したライセンスを保持し、記憶部は、デバイス部によって受信された暗号化コンテンツデータを記憶する。

【００９５】デバイス部は、バインディングライセンスを保持するとともに、配信サーバから暗号化コンテンツデータおよびライセンスを受信し、その受信したライセンスをバインディングライセンスとともに保持する。

【００９６】したがって、この発明によれば、ハードウエアによって取得したライセンスとソフトウエアによって取得したライセンスとを独立同じセキュリティレベルで管理できる。

【００９７】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【００９８】【実施の形態１】図１は、本発明によるデータ端末装置（パーソナルコンピュータ）が暗号化コン

テンツデータを取得するとともに、その取得した暗号化コンテンツデータを他のデータ端末装置（パーソナルコンピュータ）へ移動するデータ配信システムの全体構成を概念的に説明するための概略図である。

【００９９】なお、以下ではインターネットを介してデジタル音楽データを各パーソナルコンピュータのユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画像データ等を配信する場合においても適用することが可能なものである。

【０１００】図１を参照して、パーソナルコンピュータ５０は、モデム４０およびインターネット網３０を介して、各パーソナルコンピュータのユーザからの配信要求（配信リクエスト）を配信サーバ１０に送信する。著作権の存在する音楽データを管理する配信サーバ１０は、データ配信を求めてアクセスして来たパーソナルコンピュータのユーザが所有するパーソナルコンピュータ５０が正当な認証データを持つか否か、すなわち、正規のパーソナルコンピュータは充分なセキュリティレベルを備えたコンテンツ保護を行っているか否かの認証処理を行ない、正当なコンテンツ保護を行っているパーソナルコンピュータに対して所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、このような暗号化コンテンツデータおよび暗号化コンテンツデータを再生するために必要な情報としてのライセンスをパーソナルコンピュータ５０に配信する。

【０１０１】この場合、パーソナルコンピュータ５０は、モデム４０およびインターネット網３０を介して異なるセキュリティレベルによって暗号化コンテンツデータおよびライセンスを配信サーバ１０から受信して、管理することができる。すなわち、パーソナルコンピュータ５０は、ハード的にコンテンツ点準保護を実現するライセンス管理デバイスと、ソフト的にコンテンツ保護を実現するライセンス管理モジュールとを内蔵している。ライセンス管理デバイスは、アプリケーションソフトの助けを得て、配信サーバ１０からインターネット網３０等を介して暗号化コンテンツデータおよびライセンスを受信する。このライセンス管理デバイスは、暗号化コンテンツデータを再生するためのライセンスを受信するための暗号通信路を、直接、配信サーバとの間で確立し、受信したライセンスをハード的に保持するものであり、セキュリティレベルが高いものである。また、ライセンス管理モジュールも、同様に、所定の手順に従った暗号通信路を配信サーバとの間で確立し、ライセンスを受信し、暗号化して保護した上で、ハードディスク（ＨＤＤと言う）にライセンスを記録する。ライセンス管理デバイスよりも低いセキュリティレベルで暗号化コンテンツデータおよびライセンスを受信し、管理するものである。いずれの場合においても、暗号化コンテンツデータはそのままＨＤＤに記録される。ライセンス管理デバイスおよびライセンス管理モジュールについては、後に詳細に説明する。

【０１０２】以後、セキュリティレベルおよびライセンスを区別するためにメモリカード１１０あるいはライセンス管理デバイスなどのハードウエアによって機密性を保つセキュリティレベルをレベル２と呼び、レベル２のセキュリティを要求して配信サーバから送信されるライセンスをレベル２ライセンスと呼ぶことをする。同様に、ライセンス管理モジュールのようなソフトウエアによって機密性を保つセキュリティレベルをレベル１と呼び、レベル１のセキュリティレベルを要求して配信サーバから送信されるライセンスをレベル１ライセンスと呼ぶことをする。

【０１０３】さらに、図１においては、パーソナルコンピュータ５０は、ライセンス管理モジュールを使って音楽データを記録した音楽ＣＤ（Ｃｏｍｐａｃｔ　Ｄｉｓｋ）６０から取得した音楽データから、個人使用に限定したローカル使用に限定された暗号化コンテンツデータと、暗号化コンテンツデータを再生するためのライセンスとを生成することができる。この処理をリッピングと呼び、音楽ＣＤから暗号化コンテンツデータとライセンスとを取得する行為に相当する。リッピングによるローカル使用のライセンスは、その性格上、セキュリティレベルは決して高くないので、リッピングが如何なる手段でなされようともレベル１ライセンスとして扱われるものとする。リッピングの詳細については後述する。

【０１０４】またさらに、パーソナルコンピュータ５０は、ＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）ケーブル７０によって再生端末１００と接続し、配信サーバ１０から受信した暗号化コンテンツデータおよびライセンスを再生端末１００に装着されたメモリカード１１０に送信することが可能である。

【０１０５】またさらに、パーソナルコンピュータ５０は、受信した暗号化コンテンツデータおよびライセンスを通信ケーブル９０を介して、パーソナルコンピュータ８０へ送信する。

【０１０６】したがって、図１に示すデータ配信システムにおいては、パーソナルコンピュータ５０は、モデム４０およびインターネット網３０を介して配信サーバ１０から暗号化コンテンツデータとライセンスとを受信するとともに、音楽ＣＤから暗号化コンテンツデータとライセンスとを取得する。また、再生端末１００に装着されたメモリカード１１０は、パーソナルコンピュータ５０が配信サーバ１０または音楽ＣＤ６０から取得した暗号化コンテンツデータおよびライセンスを受信する。再生端末１００のユーザは、パーソナルコンピュータ５０を介することによって音楽ＣＤから暗号化コンテンツデータおよびライセンスを取得することが可能となる。

【０１０７】図１においては、たとえば携帯電話ユーザの再生端末１００には、着脱可能なメモリカード１１０が装着される構成となっている。メモリカード１１０は、再生端末１００により受信された暗号化コンテンツデータを受取り、上記配信にあたって行なわれた暗号化を復号した上で、再生端末１００中の音楽再生部（図示せず）に与える。

【０１０８】さらに、たとえば携帯電話ユーザは、再生端末１００に接続したヘッドホーン１３０等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

【０１０９】また、図１においては、パーソナルコンピュータ５０は、ライセンス管理モジュールを使って、ライセンス管理モジュールが直接管理するレベル１ライセンスを持つ暗号化コンテンツデータに限り、ライセンス管理モジュールと密接な連携を取る音楽再生プログラムを用いて再生する機能を備えることができる。レベル２ライセンスを持つ暗号化コンテンツデータの再生は、再生端末と同様な構成を持つハードウエアによって機密性を持つコンテンツ再生回路をパーソナルコンピュータに備えれば可能となる。パーソナルコンピュータにおける再生についての詳細な説明は、本出願における説明を煩略化するために省略する。

【０１１０】このような構成とすることで、充分なセキュリティレベルのコンテンツ保護機能をもつ、正規なライセンス管理デバイスあるいはライセンス管理モジュールを備えたパーソナルコンピュータでないと、配信サーバ１０からコンテンツデータの配信を受信し、パーソナルコンピュータ８０や再生端末１００へ暗号化コンテンツデータを送信することが困難な構成となる。

【０１１１】しかも、配信サーバ１０において、たとえば１曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、パーソナルコンピュータのユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、インターネット網の使用料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【０１１２】なお、図１において、再生端末１００は、配信サーバ１０と直接通信する機能を有しない再生端末を想定している。

【０１１３】図１に示したような構成においては、暗号化して配信されるコンテンツデータをパーソナルコンピュータのユーザ側で再生可能とするためにシステム上必要とされるのは、第１には、通信における暗号鍵を配信するための方式であり、さらに第２には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第３には、このように配信されたコンテンツデータの無断コピーを防止するためのコンテンツデータ保護を実現する構成である。

【０１１４】本発明の実施の形態においては、特に、配信、移動、チェックアウト、チェックイン、および再生の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびデータ再生端末（コンテンツを再生できるデータ再生端末を再生端末またはパーソナルコンピュータとも言う。以下同じ））に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【０１１５】なお、以下の説明においては、配信サーバ１０から、各パーソナルコンピュータ等にコンテンツデータを伝送する処理を「配信」と称することとする。

【０１１６】図２は、図１に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【０１１７】まず、配信サーバ１０より配信されるデータについて説明する。Ｄｃは、音楽データ等のコンテンツデータである。コンテンツデータＤｃは、ライセンス鍵Ｋｃで復号可能な暗号化が施される。ライセンス鍵Ｋｃによって復号可能な暗号化が施された暗号化コンテンツデータ｛Ｄｃ｝Ｋｃがこの形式で配信サーバ１０よりパーソナルコンピュータのユーザに配布される。

【０１１８】なお、以下においては、｛Ｙ｝Ｘという表記は、データＹを、復号鍵Ｘにより復号可能な暗号化を施したことを示すものとする。

【０１１９】さらに、配信サーバ１０からは、暗号化コンテンツデータとともに、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Ｄｃ－ｉｎｆが配布される。また、ライセンスとして、ライセンス鍵Ｋｃ、配信サーバ１０からのライセンス銘等の配信を特定するための管理コードであるトランザクションＩＤが配信サーバ１０とパーソナルコンピュータ５０との間でやり取りされる。また、配信によらないライセンス、すなわち、個人使用を目的としたローカルでの使用のライセンスを特定するためにもトランザクションＩＤは使用される。配信によるものと、ローカル使用のものを区別するために、トランザクションＩＤの先頭は“０”で始まるものがローカル使用のトランザクションＩＤであり、“０”以外から始まるのものを配信によるトランザクションＩＤであるとする。さらに、ライセンスとしては、コンテンツデータＤｃを識別するためのコードであるコンテンツＩＤ、利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件ＡＣに基づいて生成される、記録装置（メモリカード、またはライセンス管理デバイス）におけるライセンスのアクセスに対する制限に関する情報であるアクセス制御情報ＡＣｍおよびデータ再生端末における制御情報である再生制御情報ＡＣｐ等が存在する。具体的には、アクセス制限情報ＡＣｍはメモリカード、ライセンス管理モジュールおよびライセ

ンス管理モジュールからのライセンスまたはライセンス鍵を外部に出力に対するにあった手の制御情報であり、再生可能回数（再生のためにライセンス鍵を出力する数）、ライセンスの移動・複製に関する制限情報およびライセンスのセキュリティレベルなどがある。再生制御情報ＡＣｐは、再生するためにコンテンツ再生回路がライセンス鍵を受取った後に、再生を制限する情報であり、再生期限、再生速度変更制限、再生範囲指定（頭分ライセンス）などがある。

【０１２０】本発明の実施の形態においては、簡単化のためアクセス制限情報ＡＣｍは再生回数の制限を行なう制御情報である再生回数（０：再生不可、１～２５４：再生可能回数、２５５：制限無し）、ライセンスの移動および複製を制限する移動複製フラグ（０：移動複製禁止・１：移動のみ可・２：移動複製可）、セキュリティレベル「１：レベル１、２：レベル２」の３項目とし、再生制御情報ＡＣｐは再生可能な期限を規定する制御情報である再生期限「ＵＴＣｔｉｍｅコード」のみを制限するものとする。ゆえに、以降では、再生制御情報ＡＣｐを再生期限ＡＣｐとも称する。

【０１２１】さらに、以後、トランザクションＩＤとコンテンツＩＤとを併せてライセンスＩＤと総称し、ライセンス鍵ＫｃとライセンスＩＤとアクセス制限情報ＡＣｍと再生期限ＡＣｐとを併せて、ライセンスと総称することとする。

【０１２２】本発明の実施の形態においては、記録装置（メモリカード、ライセンス管理デバイスおよびライセンス管理モジュール）やコンテンツデータを再生する再生端末のクラスごとに、コンテンツデータの配信、および再生を禁止することができるように禁止クラスリストＣＲＬ（Ｃｌａｓｓ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）の運用を行なう。以下では、必要に応じて記号ＣＲＬによって禁止クラスリスト内のデータを表わすこともある。

【０１２３】禁止クラスリスト関連情報には、ライセンスの配信、移動、チェックアウト、および再生が禁止される再生端末、メモリカード、ライセンス管理モジュール、およびライセンス管理デバイスのクラスをリストアップした禁止クラスリストデータＣＲＬが含まれる。コンテンツデータ保護に関わるライセンスの管理・審積およびライセンスを受けて再生を行なう全ての機器およびプログラムがリストアップの対象となる。

【０１２４】禁止クラスリストデータＣＲＬは、配信サーバ１０内で管理されるとともに、メモリカードや、ライセンス管理モジュールによってパーソナルコンピュータ５０内のハードディスク（ＨＤＤ）またはライセンス管理デバイス内にも記録保持される。このような禁止クラスリストは、随時バージョンアップしデータを更新していく必要があるが、データの変更については、基本的には暗号化コンテンツデータおよび／またはライセンス鍵等のライセンスを配信する際に、パーソナルコンピュータ（ライセンス管理デバイスまたはライセンス管理モジュール）から受取った禁止クラスリストの更新日時を判断し、更新されていないと判断されたとき、更新された禁止クラスリストをパーソナルコンピュータに配信する。また、ライセンス管理モジュール、ライセンス管理デバイス、および再生端末１００の間でも禁止クラスリストはやり取りされ、そのデータ変更も上述したのと同じである。さらに、禁止クラスリストの変更については、変更点のみを反映した差分データＣＲＬを配信サーバ１０側より発生して、これに応じてメモリカード、ハードディスク、およびライセンス管理デバイス内の禁止クラスリストＣＲＬに追加する構成とすることも可能である。また、禁止クラスリストの更新日時ＣＲＬｄａｔｅについては、メモリカード、ハードディスク、およびライセンス管理デバイス内に記録された禁止クラスリストＣＲＬ内に記録されていて、これを配信サーバ１０側で確認することによってバージョン管理を実行する。差分データＣＲＬ更新日時ＣＲＬｄａｔｅも含まれる。

【０１２５】このように、禁止クラスリストＣＲＬを、配信サーバのみならずメモリカードまたはパーソナルコンピュータ内においても保持運用することによって、クラス固有すなわち、再生端末およびメモリカードまたはパーソナルコンピュータ（ライセンス管理デバイスまたはライセンス管理モジュール）の種類に固有の復号鍵が破られた、再生端末およびメモリカードまたはパーソナルコンピュータへのライセンス鍵の供給を禁止する。このため、再生端末ではコンテンツデータの再生が、メモリカード、ライセンス管理モジュール、およびライセンス管理デバイスでは新たなライセンスを受信することができなくなる。

【０１２６】このように、メモリカードまたはライセンス管理デバイス内の、あるいはライセンス管理モジュールが管理するＨＤＤ内の禁止クラスリストＣＲＬは配信時に逐次データを更新する構成とする。また、メモリカード、ライセンス管理モジュール、およびライセンス管理デバイスにおける禁止クラスリストＣＲＬの管理は、上位レベルとは独立にメモリカード、ライセンス管理デバイス、およびライセンス管理モジュールによって制御されるハードディスクでタンパーレジスタントモジュール（Ｔａｍｐｅｒ　Ｒｅｓｉｓｔａｎｔ　Ｍｏｄｕｌｅ）に記録する。メモリカードまたはライセンス管理デバイス内では、ライセンスと同様に、ハード的に機密性を保証する高いレベルのタンパレジスタントモジュールによって記録され、ライセンス管理モジュールが管理するＨＤＤ内に記録された禁止クラスリストＣＲＬの管理は、暗号処理によって少なくとも改ざん防止処置が行われてパーソナルコンピュータのＨＤＤ等に記録される。言いかえれば、ソフトウエアによってその機密性が保証された低いレベルのタンパーレジスタントジュールによって

記録される。いずれにしても、ファイルシステムやアプリケーションプログラム等によって上位レベルから禁止クラスリストデータＣＲＬを改ざんすることが不可能な構成とする。この結果、データに関する著作権保護をより強固なものとすることができる。

【０１２７】図３は、図１に示すデータ配信システムにおいて使用される認証のためのデータ、情報等の特性を説明する図である。

【０１２８】再生端末、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールには固有の公開暗号鍵ＫＰｐｙおよびＫＰｍｗがそれぞれ設けられ、公開暗号鍵ＫＰｐｙおよびＫＰｍｗは再生端末に固有の秘密復号鍵Ｋｐｙおよびメモリカード、ライセンス管理デバイス、およびライセンス管理モジュールに固有の秘密復号鍵Ｋｍｗによってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、再生端末、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称し、これらの公開暗号鍵をクラス公開暗号鍵、秘密復号鍵をクラス秘密復号鍵、クラス鍵を共有する単位をクラスと称する。クラスは、製造会社や製品の種類、製造時のロット等によって異なる。

【０１２９】また、コンテンツ再生デバイス（再生端末）のクラス証明書としてＣｐｙが設けられ、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールのクラス証明書としてＣｍｗが設けられる。

【０１３０】これらのクラス証明書は、コンテンツ再生デバイス、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールのクラスごとに異なる情報を有する。タンパーレジスタントモジュールが破られたり、クラス鍵による暗号が破られた、すなわち、クラス秘密復号鍵が取得されたクラス鍵に対しては、禁止クラスリストにリストアップされてライセンスの送信の禁止対象となる。

【０１３１】これらのコンテンツ再生デバイス、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールに固有のクラス公開暗号鍵およびクラス証明書は、認証データ｛ＫＰｐｙ／／Ｃｐｙ｝ＫＰａの形式または認証データ｛ＫＰｍｗ／／Ｃｍｗ｝ＫＰａの形式で、出荷時にデータ再生デバイス（再生端末）、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールにそれぞれ記録される。後ほど詳細に説明するが、ＫＰａは配信システム全体で共通の公開認証鍵である。

【０１３２】さらに、メモリカード１１０、ライセンス管理デバイス、およびライセンス管理モジュール内のデータ処理を管理するための鍵として、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールという媒体または管理ソフトウエアごとに設定される公開暗号鍵ＫＰｍｃｘと、公開暗号鍵ＫＰｍｃｘで暗号化されたデータを復号することが可能なそれぞれに固有の秘密復号鍵Ｋｍｃｘが存在する。このメモリカード毎に予測な公開暗号鍵および秘密復号鍵を総称して個別鍵と称し、公開暗号鍵ＫＰｍｃｘを個別公開暗号鍵、秘密復号鍵Ｋｍｃｘを個別秘密復号鍵と称する。

【０１３３】メモリカード外とメモリカード間でのデータ授受、またはライセンス管理デバイス外とライセンス管理デバイス間でのデータ授受、またはライセンス管理モジュール外とライセンス管理モジュール間でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、および再生が行なわれるごとに配信サーバ１０、再生端末１００、メモリカード１１０、ライセンス管理デバイス、ライセンス管理モジュールにおいて生成される共通鍵Ｋｓ１～Ｋｓ３が用いられる。

【０１３４】ここで、共通鍵Ｋｓ１～Ｋｓ３は、配信サーバ、再生端末もしくはメモリカードもしくはライセンス管理デバイスもしくはライセンス管理モジュール間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ｋｓ１～Ｋｓ３を「セッションキー」とも呼ぶことをする。

【０１３５】これらのセッションキーＫｓ１～Ｋｓ３は、各セッションごとに固有の値を有することにより、配信サーバ、再生端末、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールによって管理される。具体的には、セッションキーＫｓ１は、配信サーバによって配信セッションごとに発生される。セッションキーＫｓ２は、メモリカード、ライセンス管理デバイス、ライセンス管理モジュールによって配信セッションおよび再生セッションごとに発生し、セッションキーＫｓ３は、再生端末において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでライセンス鍵等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【０１３６】図４は、ソフトウエア（ライセンス管理モジュール）によって取得した暗号化コンテンツデータおよびライセンスを他のパーソナルコンピュータへ移動可能とするためにライセンス管理デバイスに関連付けて暗号化し管理するために必要なバインディングライセンスと、ソフトウエアによって取得した暗号化コンテンツデータおよびライセンスをメモリカード１１０へ貸出すチェックアウトセッションにおけるチェックアウト管理情報とを示したものである。

【０１３７】バインディングライセンスは、暗号化コンテンツデータを再生するためのレベル１ライセンスと、ライセンスのチェックアウトに関する情報を暗号化し

て、ソフトタンパレジスタントモジュールを実現するための共通鍵であるバインディング鍵と、バインディングライセンスに対する制御情報であるＡＣｍｂ，ＡＣｐｂと、バインディングライセンス用のトランザクションＩＤであるトランザクションＩＤｂと、バインディングＩＤ用のダミーであるコンテンツＩＤｂと、トランザクションＩＤｂとコンテンツＩＤｂとの総称であるバインディングＩＤとから成る。すなわち、ライセンス管理デバイスにライセンスとして記録することを前提としているため、ライセンスと同じ構成を持つ。

【０１３８】バインディング鍵Ｋｂは、ソフトウエアによって取得された暗号化コンテンツデータのライセンスを管理するものであり、ハードウエアによって保持される。そして、ハードウエアによって保持されたバインディング鍵Ｋｂによらなければライセンスを取出すことができないものである。また、制御情報ＡＣｍｂ，ＡＣｐｂは、暗号化コンテンツデータを再生するライセンスに含まれるＡＣｍ，ＡＣｐに相当するもので、固定値を持つ。ＡＣｍｂは、ライセンスの再生回数制限無し、移動複製禁止、かつ、セキュリティレベル１を表し、ＡＣｐｂは、再生期限が無期限であることを表す。

【０１３９】チェックアウト管理情報は、チェックアウト可能数と、チェックアウト先個別ＩＤと、チェックアウト時トランザクションＩＤとから成る。チェックアウト可能数は、暗号化コンテンツデータを貸出すことができる回数を示すものであり、暗号化コンテンツデータをチェックアウトする毎に数値が１づつ減じられ、暗号化コンテンツデータをチェックインする毎に数値が１づつ増加されるものである。また、チェックアウト先個別ＩＤは、暗号化コンテンツデータをチェックアウトするメモリカードを特定する識別情報であり、メモリカードが保持する個別公開暗号鍵ＫＰｍｃｘが該当する。チェックアウト時トランザクションＩＤは、チェックアウトするときに用いられるローカル使用のトランザクションＩＤである。

【０１４０】図５は、図１に示した配信サーバ１０の構成を示す概略ブロック図である。配信サーバ１０は、コンテンツデータを所定の方式に従って暗号化したデータや、コンテンツＩＤ等の配信情報を保持するための情報データベース３０４と、パーソナルコンピュータの各ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース３０２と、禁止クラスリストＣＲＬを管理するＣＲＬデータベース３０６と、情報データベース３０４に保持されたコンテンツデータのメニューを保持するメニューデータベース３０７と、ライセンスの配信ごとにコンテンツデータおよびライセンス鍵等の配信を特定するトランザクションＩＤの配信に関する記録して、保持する配信記録データベース３０８と、情報データベース３０４、課金データベース３０２、ＣＲＬデータベース３０６、メニューデータベース３０７、および配信記録データベース３０８からのデータをバスＢＳ１を介して受取り、所定の処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリア２０とデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。

【０１４１】データ処理部３１０は、バスＢＳ１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１５と、配信制御部３１５に制御されて、配信セッション時にセッションキーＫｓ１を発生するためのセッションキー発生部３１６と、ライセンス管理デバイス、およびライセンス管理モジュールから送られてきた認証のための認証データ（ＫＰｍｗ／／Ｃｍｗ）ＫＰａを復号するための公開認証鍵ＫＰａを保持する認証鍵保持部３１３と、ライセンス管理デバイス、およびライセンス管理モジュールから送られてきた認証のための認証データ（ＫＰｍｗ／／Ｃｍｗ）ＫＰａを通信装置３５０およびバスＢＳ１を介して受けて、認証鍵保持部３１３からの公開認証鍵ＫＰａによって復号処理を行なう復号処理部３１２と、セッションキー発生部３１６より生成されたセッションキーＫｓ１を復号処理部３１２によって得られたクラス公開暗号鍵ＫＰｍｗを用いて暗号化して、バスＢＳ１に出力するための暗号化処理部３１８と、セッションキーＫｓ１によって暗号化された上で送信されたデータをバスＢＳ１より受けて、復号処理を行なう復号処理部３２０とを含む。

【０１４２】データ処理部３１０は、さらに、配信制御部３１５から与えられるライセンス鍵Ｋｃおよびアクセス制限情報ＡＣｍを、復号処理部３２０によって得られたメモリカード、ライセンス管理デバイス、およびライセンス管理モジュールの個別公開暗号鍵ＫＰｍｃｘによって暗号化するための暗号化処理部３２６と、暗号化処理部３２６の出力を、復号処理部３２０から与えられるセッションキーＫｓ２によってさらに暗号化してバスＢＳ１に出力するための暗号化処理部３２８とを含む。

【０１４３】配信サーバが保持する認証鍵は、配信サーバが配信しようとするライセンスの要求する受信側のセキュリティレベルによって異なる。セキュリティレベル２を要求するレベル２ライセンスを配信する配信サーバにあっては、セキュリティレベルがレベル２の機器が送信してくる認証データに対して認証処理が可能な認証鍵ＫＰａ２を保持する。また、配信しようとするライセンスがセキュリティレベル１を要求するレベル１ライセンスを配信する配信サーバにあっては、セキュリティレベルがレベル２の機器およびセキュリティレベルがレベル１の機器のいずれに対しても配信可能であるため、レベル２およびレベル１のそれぞれに対応した認証鍵ＫＰａ２およびＫＰａ１を保持し、相手のレベルに応じて使い分けることになる。さらには、送信された認証データが必要とする認証鍵は、クラス証明書Ｃｍｗの認証データとして暗号化されても、なお、平文として維持される領

城に記載され配信サーバ１０の配信制御部３１５が、復号処理部３１２にて復号前に容易に認証鍵を特定できる構成となっている。２つの認証鍵を区別するためにレベル２に対応した認証鍵ＫＰａ２をレベル２認証鍵ＫＰａ２、レベル１に対応した認証鍵ＫＰａ１をレベル１認証鍵ＫＰａ１と称し、総じて認証鍵ＫＰａと称する。

【０１４４】配信サーバ１０の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【０１４５】図６は、図１に示したパーソナルコンピュータ５０の構成を説明するための概略ブロック図である。パーソナルコンピュータ５０は、パーソナルコンピュータ５０の各部のデータ授受を行なうためのバスＢＳ２と、パーソナルコンピュータ内を制御すると共に、各種のプログラムを実行するためのコントローラ（ＣＰＵ）５１０と、データバスＢＳ２と、データバスＢＳ２に接続され、プログラムやデータを記録し、蓄積しておくための大容量記録装置であるハードディスク（ＨＤＤ）５３０およびＣＤ－ＲＯＭドライブ５４０と、ユーザからの指示を入力するためのキーボード５６０と、各種の情報を視覚的にユーザに与えるためのディスプレイ５７０とを含む。

【０１４６】パーソナルコンピュータ５０は、さらに、暗号化コンテンツデータおよびライセンスを再生端末１００等に通信する際にコントローラ５１０と端子５８０との間でデータの授受を制御するためのＵＳＢインタフェース５５０と、ＵＳＢケーブル７０を接続するための端子５８０と、配信サーバ１０とインタネット網３０およびモデム４０を介して通信する際にコントローラ５１０と端子５８５との間でデータの授受を制御するための シリアルインタフェース５５５と、ケーブルによってモデム４０と接続するための端子５８５とを含む。

【０１４７】コントローラ５１０は、アプリケーションプログラムを実行することで、インターネット網３０を介してライセンス管理デバイス５２０またはライセンス管理モジュール５１１に暗号化コンテンツデータ等を配信サーバ１０から受信するために、配信サーバ１０との間でデータの授受を制御するとともに、ＣＤ－ＲＯＭドライブ５４０を介して音楽ＣＤからリッピングによって暗号化コンテンツデータおよびライセンスを取得する際の制御を行なう。

【０１４８】さらに、パーソナルコンピュータ５０は、配信サーバ１０からの暗号化コンテンツデータおよびライセンスの受信を行なう際に配信サーバ１０との間で各種の鍵のやり取りを行ない、配信された暗号化コンテンツデータを再生するためのライセンスをハード的に管理するライセンス管理デバイス５２０と、コントローラ５１０にて実行されるプログラムであって、配信サーバ１０からの暗号化コンテンツデータおよびレベル１ライセンスの受信をプログラムによって実行し、受信したライセンスに独自の暗号化を施した専用ライセンスを生成するコンテンツ管理モジュール５１１とを含む。

【０１４９】ライセンス管理デバイス５２０は、暗号化コンテンツデータおよびライセンスを配信サーバ１０から受信する際のデータの授受をハード的に行ない、受信したライセンスをハード的に管理するものであるため、高いセキュリティレベルを要求するレベル２のライセンスを扱うことが出る。一方、ライセンス管理モジュール５１１は、暗号化コンテンツデータおよびライセンスを配信サーバ１０から受信する際のデータの授受をコンコローラ５１０にて実行されるプログラムを用いてソフト的に行ない、ライセンスの受信を、また、音楽ＣＤからリッピングによってローカル使用の暗号化コンテンツデータおよびライセンスの生成を行い、取得したライセンスに対して暗号処理などを施して保護し、ＨＤＤ５３０に蓄積して管理するものであるため、ライセンス管理デバイス５２０よりもセキュリティレベルが低い、レベル１ライセンスのみを扱う。なお、高いセキュリティレベルがレベル２である場合にはレベル１ライセンスも扱えることは言うまでもない。

【０１５０】このように、パーソナルコンピュータ５０は、配信サーバ１０からインターネット網３０を介して暗号化コンテンツデータおよびライセンスを受信するためのライセンス管理モジュール５１１およびライセンス管理デバイス５２０と、音楽ＣＤからリッピングによって暗号化コンテンツデータおよびライセンスを取得するためのＣＤ－ＲＯＭドライブ５４０とを内蔵するものである。

【０１５１】図７は、図１に示した再生端末１００の構成を説明するための概略ブロック図である。

【０１５２】再生端末１００は、再生端末１００の各部のデータ授受を行なうためのバスＢＳ３と、バスＢＳ３を介して再生端末１００の動作を制御するためのコントローラ１１０６と、外部からの指示を再生端末１００に与えるための操作パネル１１０８と、コントローラ１１０６等から出力される情報を携帯電話ユーザに視覚情報として与えるための表示パネル１１１０とを含む。

【０１５３】再生端末１００は、さらに、配信サーバ１０からのコンテンツデータ（音楽データ）を記憶しかつ復号化処理するための着脱可能なメモリカード１１０と、メモリカード１１０とバスＢＳ３との間のデータの授受を制御するためのメモリインタフェース１２００と、パーソナルコンピュータ５０から暗号化コンテンツデータおよびライセンスを受信する際にバスＢＳ３と端子１１１４との間のデータ授受を制御するためのＵＳＢインタフェース１１１２と、ＵＳＢケーブル７０を接続するための端子１１１４とを含む。

【０１５４】再生端末１００は、さらに、再生端末の種類（クラス）ごとにそれぞれ設定される、クラス公開暗号鍵ＫＰｐ１およびクラス証明書Ｃｐ１をクラス公開認

証鍵ＫＰａで復号することでその正当性を認証できる状態に暗号化した認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａ２を保持する認証データ保持部１５００を含む。ここで、再生端末１００のクラスｙは、ｙ＝１であるとする。また、再生端末は、ハード的に機密性を保持できるコンテンツ再生デバイスを用いて再生を提供する機器であるためセキュリティレベルはレベル２である。

【０１５５】再生端末１００は、さらに、再生端末（コンテンツ再生デバイス）のクラス秘密復号鍵であるＫｐ１を保持するＫｐ１保持部１５０２と、バスＢＳ３から受けたデータをＫｐ１によって復号しメモリカード１１０によって発生されたセッションキーＫｓ２を得る復号処理部１５０４とを含む。

【０１５６】再生端末１００は、さらに、メモリカード１１０に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード１１０との間でバスＢＳ３上においやり取りされるデータを暗号化するためのセッションキーＫｓ３を乱数等により発生するセッションキー発生部１５０８と、暗号化コンテンツデータの再生セッションにおいてメモリカード１１０からライセンス鍵Ｋｃおよび再生期限ＡＣｐを受取る際に、セッションキー発生部１５０８により発生されたセッションキーＫｓ３を復号処理部１５０４によって得られたセッションキーＫｓ２によって暗号化しバスＢＳ３に出力する暗号化処理部１５０６とを含む。

【０１５７】再生端末１００は、さらに、バスＢＳ３上のデータをセッションキーＫｓ３によって復号して、ライセンス鍵Ｋｃおよび再生期限ＡＣｐを出力する復号処理部１５１０と、バスＢＳ３より暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを受けて、復号処理部１５１０より取得したライセンス鍵Ｋｃによって復号しコンテンツデータを出力する復号処理部１５１６と、復号処理部１５１６の出力を受けてコンテンツデータを再生するための音楽再生部１５１８と、音楽再生部１５１８の出力をディジタル信号からアナログ信号に変換するＤＡ変換器１５１９と、ＤＡ変換器１５１９の出力をヘッドホーンなどの外部出力装置（図示省略）へ出力するための端子１５３０とを含む。

【０１５８】なお、図７においては、点線で囲んだ領域は暗号化コンテンツデータを復号して音楽データを再生するコンテンツ再生デバイス１５５０を構成する。また、図７においては、説明の簡潔化のため、再生端末のうち本発明の音楽データの再生にかかわるブロックのみを記載し、再生端末が本来備えている通話機能に関するブロックについては、一部記載を省略している。

【０１５９】再生端末１００の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【０１６０】図８は、メモリカード１１０の構成を説明するための概略ブロック図である。既に説明したように、メモリカードに固有の公開暗号鍵および秘密復号鍵として、ＫＰｍｗおよびＫｍｗが設けられ、メモリカードのクラス証明書Ｃｍｗが設けられるが、メモリカード１１０においては、メモリカードのクラスを識別する自然数ｗ＝３で、メモリカードを識別する自然数ｘ＝４でそれぞれ表わされるものとする。また、メモリカード１１０は、ハード的に機密性を保持する機器であるためセキュリティレベルは２である。

【０１６１】したがって、メモリカード１１０は、認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２を保持する認証データ保持部１４００と、メモリカードごとに設定される固有の復号鍵である個別秘密復号鍵Ｋｍｃ４を保持するＫｍｃ保持部１４０２と、メモリカードの種類ごとに設定される固有のクラス秘密復号鍵Ｋｍ３を保持するＫｍ保持部１４２１と、個別秘密復号鍵Ｋｍｃ４によって復号可能な公開暗号鍵ＫＰｍｃ４を保持するＫＰｍｃ保持部１４１６とを含む。

【０１６２】このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンス鍵の管理をメモリカード単位で実行することが可能になる。

【０１６３】メモリカード１１０は、さらに、メモリインタフェース１２００との間で信号を端子１４２６を介して授受するインタフェース１４２４と、インタフェース１４２４との間で信号をやり取りするバスＢＳ４と、バスＢＳ４にインタフェース１４２４から与えられるデータから、メモリカードの種類ごとに固有のクラス秘密復号鍵Ｋｍ３をＫｍ保持部１４２１から受けて、配信サーバ１０が配信セッションにおいて生成したセッションキーＫｓ１を独点Ｐａに出力する復号処理部１４２２と、ＫＰａ保持部１４１４からレベル２認証鍵ＫＰａ２を受けて、バスＢＳ４に与えられるデータからレベル２認証鍵ＫＰａ２による復号処理を実行して復号結果と得られたクラス証明書をコントローラ１４２０に、得られたクラス公開鍵を暗号化処理部１４１０に出力する復号処理部１４０８と、切換スイッチ１４４２によって選択的に与えられる鍵によって、切換スイッチ１４４６によって選択的に与えられるデータを暗号化してバスＢＳ４に出力する暗号化処理部１４０６とを含む。

【０１６４】メモリカード１１０は、さらに、各セッションにおいてセッションキーＫｓ２を発生するセッションキー発生部１４１８と、セッションキー発生部１４１８の出力したセッションキーＫｓ２を復号処理部１４０８によって得られるクラス公開暗号鍵ＫＰｐもしくはＫＰｍｗによって暗号化してバスＢＳ４に送出する暗号化処理部１４１０と、バスＢＳ４よりセッションキーＫｓ２によって暗号化されたデータを受けてセッションキー発生部１４１８より得たセッションキーＫｓ２によって復号する復号処理部１４１２と、暗号化コンテンツデ

ータの再生セッションにおいてメモリ１４１５から読出されたライセンス鍵Ｋｃおよび再生期限ＡＣｐを、復号処理部１４１２で復号された他のメモリカード１１０に固有の個別公開暗号鍵ＫＰｍｃｘ（≠４）で暗号化する暗号処理部１４１７とを含む。

【０１６５】メモリカード１１０は、さらに、バスＢＳ４上のデータを個別公開暗号鍵ＫＰｍｃ４と対をなすメモリカード１１０固有の個別秘密復号鍵Ｋｍｃ４によって復号するための復号処理部１４０４と、禁止クラスリストデータＣＲＬと、暗号化コンテンツデータ〔Ｄｃ〕Ｋｃと、暗号化コンテンツデータ〔Ｄｃ〕Ｋｃを再生するためのライセンス（Ｋｃ，ＡＣｐ，ＡＣｍ，ライセンスＩＤ）と、付加情報Ｄａｔａ－ｉｎｆｏ、暗号化コンテンツデータの再生リストファイルと、ライセンスを管理するためのライセンス管理ファイルとをバスＢＳ４より受けて格納するためのメモリ１４１５とを含む。メモリ１４１５は、例えば半導体メモリによって構成される。また、メモリ１５１５は、禁止クラスリストＣＲＬを記録するためのＣＲＬ領域１４１５Ａと、ライセンスを記録するライセンス領域１４１５Ｂと、暗号化コンテンツデータ〔Ｄｃ〕Ｋｃ、暗号化コンテンツデータの関連情報Ｄｃ－ｉｎｆ、メモリカードに記録された暗号化コンテンツデータやライセンスをアクセスするための基本的な情報を記録する再生リストファイル、およびライセンスを管理するために必要な情報を暗号化コンテンツデータごとに記録するライセンス管理ファイルを記録する外部から直接アクセスが可能なデータ領域１４１５Ｃとから成る。ライセンス管理ファイルおよび再生リストファイルの詳細については後述する。

【０１６６】また、ライセンス領域１４１５Ｂは、ライセンス（コンテンツ鍵Ｋｃ、再生制御情報ＡＣｐ、アクセス制限情報ＡＣｍ、ライセンスＩＤ）を記録するためにエントリと呼ばれるライセンス専用の記録単位でライセンスを格納する。ライセンスに対してアクセスする場合には、ライセンスが格納されている、あるいは、ライセンスを記録したいエントリをエントリ番号によって指定する構成になっている。

【０１６７】メモリカード１１０は、さらに、バスＢＳ４を介して外部との間でデータ授受を行ない、バスＢＳ４との間で再生情報等を受けて、メモリカード１１０の動作を制御するためのコントローラ１４２０とを含む。

【０１６８】なお、データ領域１４１５Ｃを除く全ての構成は、耐タンパモジュール領域に構成される。

【０１６９】図９は、パーソナルコンピュータ５０に内蔵されたライセンス管理デバイス５２０の構成を示す概略ブロック図である。ライセンス管理デバイス５２０は、メモカード１１０におけるデータ領域１４１５Ｃに相当する領域を必要としない点、インタフェース１４２４の機能および端子１４２６の形状が異なるインタフェース５２２４と端子５２２６とを備える点が異なるのみで、基本的にメモリカード１１０と同じ構成から成る。ライセンス管理デバイス５２０の認証データ保持部５２００、Ｋｍｃ保持部５２０２、復号処理部５２０４、暗号処理部５２０６、復号処理部５２０８、暗号処理部５２１０、復号処理部５２１２、ＫＰａ保持部５２１４、ＫＰｍｃ保持部５２１６、暗号処理部５２１７、セッションキー発生部５２１８、コントローラ５２２０、Ｋｍ保持部５２２１、復号処理部５２２２、インタフェース５２２４、端子５２２６、切換スイッチ５２４２、５２４６は、それぞれ、メモリカード１１０の認証データ保持部１４００、Ｋｍｃ保持部１４０２、復号処理部１４０４、暗号処理部１４０６、復号処理部１４０８、暗号処理部１４１０、復号処理部１４１２、ＫＰａ保持部１４１４、ＫＰｍｃ保持部１４１６、暗号処理部１４１７、セッションキー発生部１４１８、コントローラ１４２０、Ｋｍ保持部１４２１、復号処理部１４２２、切換スイッチ１４４２、１４４６と同じである。ただし、認証データ保持部５２００は、認証データ〔ＫＰｍ７／／Ｃｍ７〕ＫＰａ２を保持し、ＫＰｍｃ保持部５２１６は、個別公開暗号鍵ＫＰｍ８を保持し、Ｋｍ保持部５２０２は、クラス秘密復号鍵Ｋｍ７を保持し、Ｋｍｃ保持部５２２１は、個別秘密復号鍵Ｋｍｃ８を保持する。ライセンス管理デバイス５２０のクラスを表す自然数ｗはｗ＝７であり、ライセンス管理デバイス５２０を識別するための自然数ｘはｘ＝８であるとする。

【０１７０】ライセンス管理デバイス５２０は、禁止クラスリストＣＲＬとライセンス（Ｋｃ，ＡＣｍ，ライセンスＩＤ）とを記録するメモリ５２１５を、メモリカード１１０のメモリ１４１５に代えて含む。メモリ５２１５は、禁止クラスリストＣＲＬを記録したＣＲＬ領域５２１５Ａと、ライセンスを記録したライセンス領域５２１５Ｂとから成る。

【０１７１】さらに、ライセンス管理デバイス５２０は、ライセンス管理モジュール５１１が利用するバインディングライセンスを保持する必要がある。したがって、ＫＰａ保持部５２１４は、２つの認証鍵ＫＰａ２およびＫＰａ１を保持する。異なるレベルからの制御については、後ほどフローチャートを使用して詳細に説明する。

【０１７２】更に、ライセンス管理モジュール５１１はライセンスを管理するプログラムであり、セキュリティレベルは１である。また、ライセンス管理モジュール５１１は、ライセンス管理デバイス５２０とほぼ同一の構成を持つ管理プログラムなのでライセンス管理モジュール５１１のクラスを表す自然数ｗはｗ＝５であり、ライセンス管理デバイス５２０を識別するための自然数ｘはｘ＝６であるとする。したがって、ライセンス管理モジュール５１１は、認証データ〔ＫＰｍ５／／Ｃｍ５〕ＫＰａ１、個別公開暗号鍵ＫＰｍ６、クラス秘密復号鍵Ｋｍ５、個別秘密復号鍵Ｋｍｃ６を保持する。また、２つ

の認証鍵ＫＰａ２およびＫＰａ１を保持する。

【０１７３】以下、図１に示すデータ配信システムにおける各セッションの動作について説明する。

【０１７４】［初期化］パーソナルコンピュータ５０が配信サーバ１０から暗号化コンテンツデータおよびライセンスの配信を受ける前に行なわれる初期化について説明する。

【０１７５】図１０～図１２は、パーソナルコンピュータ５０が暗号化コンテンツデータおよびライセンスを配信サーバ１０から受信する前に行なわれる初期化を説明するための第１～第３のフローチャートである。

【０１７６】図１０を参照して、バイディングライセンスの生成がキーボード６６０を介してリクエストされると（ステップＳ１０）、ライセンス管理モジュール５１１は、バインディング鍵Ｋｂを生成し（ステップＳ１２）、次いで、トランザクションＩＤｂ、コンテンツＩＤｂ、所定の制御情報ＡＣｍｂおよびＡＣｐｂを生成する（ステップＳ１４）。ステップＳ１２，Ｓ１４はバインディングライセンスの生成処理である。

【０１７７】そして、ライセンス管理モジュール５１１は、ライセンス管理デバイス５２０に対してパスＢＳ２を介して認証データの出力を指示する（ステップＳ１６）。

【０１７８】そうすると、ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６、インタフェース５２２４、およびパスＢＳ５を介して認証データの出力指示を受取り、認証データ保持部５２００からパスＢＳ５を介して認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａ２を取得し、パスＢＳ５、インタフェース５２２４および端子５２２６を介して認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａ２を出力する（ステップＳ１８）。ライセンス管理モジュール５１１は、パスＢＳ２を介して認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａ２を受信し（ステップＳ２０）、認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａをレベル２認証鍵ＫＰａ２によって復号する（ステップＳ２２）。

【０１７９】ライセンス管理モジュール５１１は、復号処理結果から、処理が正常に行なわれたか否か、すなわち、ライセンス管理デバイス５２０が正規のライセンス管デバイスからの公開暗号鍵ＫＰｍ７と証明書Ｃｍ７とを保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ２４）。正当な認証データであると判断された場合、ライセンス管理モジュール５１１は、公開暗号鍵ＫＰｍ７および証明書Ｃｍ７を承認し、受理する。そして、次の処理（ステップＳ２６）へ移行する。正当な認証データでない場合には、非承認とし、公開暗号鍵ＫＰｍ７および証明書Ｃｍ７を受理しないで処理を終了する（ステップＳ６８）。

【０１８０】認証の結果、正規の機器であることが認識されると、ライセンス管理モジュール５１１は、次に、ライセンス管理デバイスのクラス証明書Ｃｍ７が禁止クラスリストＣＲＬにリストアップされているかどうかをハードディスク（ＨＤＤ）５３０に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで初期化を終了する（ステップＳ６８）。

【０１８１】一方、ライセンス管理デバイス５２０のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップＳ２６）。

【０１８２】認証の結果、正当な認証データを持つライセンス管理デバイスからのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、ライセンス管理モジュール５１１は、セッションキーＫｓ２ａを生成する（ステップＳ２８）。

【０１８３】図１１を参照して、ライセンス管理モジュール５１１は、セッションキーＫｓ２ａをクラス公開暗号鍵ＫＰｍ７によって暗号化して暗号化データ｛Ｋｓ２ａ｝Ｋｍ７を生成し（ステップＳ３０）、暗号化データ｛Ｋｓ２ａ｝Ｋｍ７をパスＢＳ２を介してライセンス管理デバイス５２０へ出力する（ステップＳ３２）。ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６、インタフェース５２２４、およびパスＢＳ５を介して暗号化データ｛Ｋｓ２ａ｝Ｋｍ７を受信してセッションキーＫｓ２ａを復号する（ステップＳ３４）。コントローラ５２２０は、セッションキーＫｓ２ａを受理したことに伴い、セッションキー発生部５２１８を制御してセッションキーＫｓ２ｂを発生させる。そうすると、セッションキー発生部５２１８は、セッションキーＫｓ２ｂを生成し（ステップＳ３６）、コントローラ５２２０は、パスＢＳ５を介してメモリ５２１５のＣＲＬ領域５２１５Ａから禁止クラスリストＣＲＬの更新日時ＣＲＬｄａｔｅを取得し、その取得した更新日時ＣＲＬｄａｔｅをパスＢＳ５を介して切換スイッチ５２４６へ出力する（ステップＳ３８）。そすると、暗号処理部５２０６は、切換スイッチ５２４６を順次切換えることによって受取ったセッションキーＫｓ２ｂ、個別公開暗号鍵ＫＰｍｃ８および更新日時ＣＲＬｄａｔｅを復号処理部５２２２からセッションキーＫｓ２ａによって暗号化する。コントローラ５２２０は、パスＢＳ５上の暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ８／／ＣＲＬｄａｔｅ｝Ｋｓ２ａをインタフェース５２２４および端子５２２６を介して出力する（ステップＳ４０）。

【０１８４】ライセンス管理モジュール５１１は、パスＢＳ２を介して暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ８／／ＣＲＬｄａｔｅ｝Ｋｓ２ａを受取り、暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ８／／ＣＲＬｄａｔｅ｝Ｋｓ２

ａをセッションキーＫｓ２ａによって復号してセッションキーＫｓ２ｂ、個別公開暗号鍵ＫＰｍｃ８、および更新日時ＣＲＬｄａｔｅを受理する（ステップＳ４２）。そして、ライセンス管理モジュール５１１は、ステップＳ１２，Ｓ１４で生成したバインディングライセンス（トランザクションＩＤｂ、コンテンツＩＤｂ、バインディング鍵Ｋｂ、および制御情報ＡＣｍｂ、ＡＣｐｂ）を公開暗号鍵ＫＰｍｃ８によって暗号化して暗号化データ｛トランザクションＩＤｂ／／コンテンツＩＤｂ／／Ｋｂ／／ＡＣｍｂ／／ＡＣｐｂ｝Ｋｍｃ８を生成する（ステップＳ４４）。

【０１８５】図１２を参照して、ライセンス管理モジュール５１１において、ライセンス管理デバイス５２０から送信された禁止クラスリストの更新日時ＣＲＬｄａｔｅがハードディスク（ＨＤＤ）５３０に保持されている禁止クラスリストＣＲＬの更新日時から、いずれが保持する禁止クラスリストが新しいかが比較される。ライセンス管理デバイス５２０の禁止クラスリストＣＲＬの方が新しいとき、ステップＳ４８へ移行する。また、逆に、ライセンス管理モジュール５１１の禁止クラスリストＣＲＬの方が新しいときはステップＳ５２へ移行する（ステップＳ４６）。

【０１８６】ライセンス管理デバイス５２０の禁止クラスリストＣＲＬの方が新しいと判断されたとき、ライセンス管理モジュール５１１は、暗号化データ｛トランザクションＩＤｂ／／コンテンツＩＤｂ／／Ｋｂ／／ＡＣｍｂ／／ＡＣｐｂ｝Ｋｍｃ８をライセンス管理デバイス５２０において発生されたセッションキーＫｓ２ｂによって暗号化を行い、暗号化データ｛｛トランザクションＩＤｂ／／コンテンツＩＤｂ／／Ｋｂ／／ＡＣｍｂ／／ＡＣｐｂ｝Ｋｍｃ８｝Ｋｓ２ｂをパスＢＳ２を介してライセンス管理デバイス５２０へ出力する（ステップＳ４８）。

【０１８７】そして、ライセンス管理デバイス５２０のコントローラ５２２０は、暗号化データ｛｛トランザクションＩＤｂ／／コンテンツＩＤｂ／／Ｋｂ／／ＡＣｍｂ／／ＡＣｐｂ｝Ｋｍｃ８｝Ｋｓ２ｂを端子５２２６およびインタフェース５２２４を介して受取り、セッションキー発生部５２１８によって発生されたセッションキーＫｓ２ｂによって復号し、｛トランザクションＩＤｂ／／コンテンツＩＤｂ／／Ｋｃ／／ＡＣｍｂ／／ＡＣｐｂ｝Ｋｍｃ８を受理する（ステップＳ５０）。その後、ステップＳ６０へ移行する。

【０１８８】一方、ライセンス管理モジュール５１１において、ライセンス管理モジュール５１１の禁止クラスリストＣＲＬの方が新しいと判断されると、ライセンス管理モジュール５１１は、ライセンス管理デバイス５２０が保持する禁止クラスリストＣＲＬを更新するため、パスＢＳ２を介してＨＤＤ５３０から更新日時ＣＲＬｄａｔｅ以降の更新分を差分ＣＲＬとして取得する（ステップＳ５２）。

【０１８９】そして、ライセンス管理モジュール５１１は、禁止クラスリストの差分ＣＲＬと暗号化データ｛トランザクションＩＤｂ／／コンテンツＩＤｂ／／Ｋｂ／／ＡＣｍｂ／／ＡＣｐｂ｝Ｋｍｃ８とを、ライセンス管理デバイス５２０において生成されたセッションキーＫｓ２ｂによって暗号化し、暗号化データ｛ＣＲＬｄａｔｅ／／｛トランザクションＩＤｂ／／コンテンツＩＤｂ／／Ｋｂ／／ＡＣｍｂ／／ＡＣｐｂ｝Ｋｍｃ８｝Ｋｓ２ｂをパスＢＳ２を介してライセンス管理デバイス５２０へ出力する（ステップＳ５４）。

【０１９０】ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６およびインタフェース５２２４を介して、パスＢＳ５に与えられた受信データを復号処理部５２１２によって復号する。復号処理部５２１２は、セッションキー発生部５２１８から与えられたセッションキーＫｓ２ｂを用いてパスＢＳ５の受信データを復号しパスＢＳ５に出力する（ステップＳ５６）。

【０１９１】この段階で、パスＢＳ５には、Ｋｍｃ保持部５２２１に保持される個別秘密復号鍵Ｋｍｃ８で復号可能な｛トランザクションＩＤｂ／／コンテンツＩＤｂ／／Ｋｂ／／ＡＣｍｂ／／ＡＣｐｂ｝Ｋｍｃ８と、差分ＣＲＬとが出力される（ステップＳ５６）。コントローラ５２２０の指示によって受理した差分ＣＲＬにしたがってメモリ５２１５内のＣＲＬ領域５２１５Ａを差分ＣＲＬに基づいて更新する（ステップＳ５８）。

【０１９２】ステップＳ４８，Ｓ５０は、送信側のライセンス管理モジュール５１１の禁止クラスリストＣＲＬより、受信側のライセンス管理デバイス５２０の禁止クラスリストＣＲＬが新しい場合のバインディング鍵Ｋｂ等のライセンス管理デバイス５２０への送信動作であり、ステップＳ５２，Ｓ５４，Ｓ５６，Ｓ５８は、受信側のライセンス管理デバイス５２０の禁止クラスリストＣＲＬより、送信側のライセンス管理モジュール５１１の禁止クラスリストＣＲＬが新しい場合のバインディング鍵Ｋｂ等のライセンス管理デバイス５２０への送信動作である。このように、ライセンス管理デバイス５２０から送られてきた禁止クラスリストの更新日時ＣＲＬｄａｔｅを比較し、受信側の禁止クラスリストＣＲＬが送信側の禁止クラスリストＣＲＬより古いとき、禁止クラスリストの差分データである差分ＣＲＬをＨＤＤ５３０から取得し、差分ＣＲＬをライセンス管理デバイス５２０に配信することによって、常に新しい禁止クラスリストＣＲＬを保持させるようにしている。

【０１９３】ステップＳ５０またはステップＳ５８の後、コントローラ５２２０の指示によって、暗号化データ｛トランザクションＩＤｂ／／コンテンツＩＤｂ／／Ｋｂ／／ＡＣｍｂ／／ＡＣｐｂ｝Ｋｍｃ８は、復号処理部５２０４において、秘密復号鍵Ｋｍｃ８によって復号され、バインディングライセンス（バインディング鍵Ｋ

ｂ、トランザクション１Ｄｂ、コンテンツＩＤｂ、制御情報ＡＣｍＺ，ＡＣｐ）が受理される（ステップＳ６０）。

【０１９４】そして、ライセンス管理モジュール５１１は、バインディングライセンスを格納するためのエントリ番号「０」をライセンス管理デバイス５２０へ入力し（ステップＳ６２）、ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６、インタフェース５２２４、およびバスＢＳ５を介してエントリー番号「０」を受取り、メモリ５２１５のライセンス領域５２１５Ｂのうち、受取ったエントリ番号「０」によって指定された領域にバインディングライセンス（トランザクションＩＤｂ、コンテンツＩＤｂ、バインディング鍵Ｋｂ、制御情報ＡＣｍｂ，ＡＣｐｂ）を格納する（ステップＳ６４）。

【０１９５】ライセンス管理モジュール５１１が、バインディング鍵Ｋｂを記録するためにライセンス管理デバイス５２０の領域を確認し、登録の準備を行なう図１０のステップ１６から図１１のステップ４２までの一連の処理を「デバイス確認処理」、バインディング鍵Ｋｂをライセンス管理デバイス５２０のライセンス領域５２１５Ｂに格納する図１１のステップＳ４４から図１２のステップＳ６４までの一連の処理を「バインディング鍵登録処理」と称する。

【０１９６】一方、ライセンス管理モジュール５１１は、機密情報（レベル１ライセンスおよびチェックアウト情報）が空な平文の機密ファイルを生成し、バインディング鍵Ｋｂによって機密ファイルを暗号化した暗号化機密ファイル１６０を生成して暗号化機密ファイル１６０をＨＤＤ５３０に記録し（ステップＳ６６）、初期化の動作を終了する（ステップＳ６８）。

【０１９７】このように、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、初期化動作において、バインディングライセンスを生成し、ライセンス管理デバイス５２０におけるメモリ５２１５のライセンス領域５２１５Ｂのうち、エントリ番号「０」によって指定される領域に生成したバインディングライセンスを格納するとともに、生成したバインディングライセンスに含まれるバインディング鍵Ｋｂによって機密ファイルを暗号化した暗号化機密ファイル１６０を生成する。そして、この暗号化機密ファイル１６０は、ライセンス管理モジュール５１１によって配信サーバ１０から受信したライセンスを格納するためのものである。また、このようにバインディング鍵Ｋｂによって機密ファイルを暗号化することによりバインディング鍵Ｋｂがないと暗号化機密ファイル１６０からライセンスを取出すことができないため、バインディング鍵Ｋｂは暗号化コンテンツデータのライセンスを管理するための共通鍵である。そして、このバインディング鍵Ｋｂはライセンス管理デバイス５２０のメモリ５２１５に格納されているため、バインディング鍵Ｋｂをハードウエアによって管理することができる。その結果、バインディング鍵Ｋｂを介してＨＤＤ５３０に記録された暗号化機密ファイル１６０でソフト的に管理される暗号化コンテンツデータのライセンスをハードウエアによって管理することになる。したがって、後述するように、ソフトウエアによって受信された暗号化コンテンツデータおよびライセンスを他のパーソナルコンピュータ８０へ移動できる。

【０１９８】［配信１］次に、図１に示すデータ配信システムにおいて、配信サーバ１０からパーソナルコンピュータ５０のライセンス管理デバイス５２０へ暗号化コンテンツデータおよびセキュリティレベル２を要求するレベル２ライセンスを配信するための動作について説明する。なお、この動作を「配信１」という。

【０１９９】図１３～図１６は、図１に示すデータ配信システムにおける暗号化コンテンツデータの購入時に発生するパーソナルコンピュータ５０に内蔵されたライセンス管理デバイス５２０への配信動作（以下、配信セッションともいう）を説明するための第１～第４のフローチャートである。

【０２００】図１３における処理以前に、パーソナルコンピュータ５０のユーザは、配信サーバ１０に対してモデム４０を介して接続し、購入を希望するコンテンツに対するコンテンツＩＤを取得していることを前提としている。

【０２０１】図１３を参照して、パーソナルコンピュータ５０のユーザからキーボード５６０を介してコンテンツＩＤの指定による配信リクエストがなされる（ステップＳ１００）。そして、キーボード５６０を介して暗号化コンテンツデータのライセンスを購入するための購入条件ＡＣが入力される（ステップＳ１０２）。つまり、選択した暗号化コンテンツデータを復号するライセンス鍵Ｋｃを購入するために、暗号化コンテンツデータのアクセス制限情報ＡＣｍ、および再生期限ＡＣｐを設定して購入条件ＡＣが入力される。

【０２０２】暗号化コンテンツデータの購入条件ＡＣが入力されると、コントローラ５１０は、バスＢＳ２を介してライセンス管理デバイス５２０へ認証データの出力指示を与える（ステップＳ１０４）。ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６、インタフェース５２２４およびバスＢＳ５を介して認証データの出力指示を受取る。そして、コントローラ５２２０は、バスＢＳ５を介して認証データ保持部５２００から認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａ２を読出し、｛ＫＰｍ７／／Ｃｍ７｝ＫＰａ２をバスＢＳ５、インタフェース５２２４および端子５２２６を介して出力する（ステップＳ１０６）。

【０２０３】パーソナルコンピュータ５０のコントローラ５１０は、ライセンス管理デバイス５２０からの認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａ２に加えて、コン

テンツＩＤ、ライセンス購入条件のデータＡＣ、および配信リクエストを配信サーバ１０に対して送信する（ステップＳ１０８）。

【０２０４】配信サーバ１０では、パーソナルコンピュータ５０から配信リクエスト、コンテンツＩＤ、認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａ２、およびライセンス購入条件のデータＡＣを受信し（ステップＳ１１０）、復号処理部３１２においてライセンス管理デバイス５２０から出力された認証データをレベル２認証鍵ＫＰａで復号処理を実行する（ステップＳ１１２）。

【０２０５】配信制御部３１５は、復号処理部３１２における復号処理結果から、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ１１４）。正当な認証データであると判断された場合、配信制御部３１５は、クラス公開暗号鍵ＫＰｍ７およびクラス証明書Ｃｍ７を承認し、受理する。そして、次の処理（ステップＳ１１６）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵ＫＰｍ７およびクラス証明書Ｃｍ７を受理しないで配信セッションを終了する（ステップＳ１９８）。仮に、レベル１からの配信要求を行っていたとすると、レベル２認証鍵ＫＰａ２では、レベル１の認証データを認証することができないためここで処理は終了する。

【０２０６】認証の結果、正規の認証データであり、クラス公開暗号鍵ＫＰｍ７およびクラス証明書Ｃｍ７を承認されると、配信制御部３１５は、次に、ライセンス管理デバイスのクラス証明書Ｃｍ７が禁止クラスリストＣＲＬにリストアップされているかどうかをＣＲＬデータベース３０６に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する（ステップＳ１９８）。

【０２０７】一方、ライセンス管理デバイス５２０のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップＳ１１６）。

【０２０８】認証の結果、正当な認証データを持つライセンス管理デバイスを備えるパーソナルコンピュータからのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、配信サーバ１０において、配信制御部３１５は、配信を特定するための管理コードであるトランザクションＩＤを生成する（ステップＳ１１８）。また、セッションキー発生部３１６は、配信のためのセッションキーＫｓ１を生成する（ステップＳ１２０）。セッションキーＫｓ１は、復号処理部３１２によって得られたライセンス管理デバイス５２０に対応するクラス公開暗号鍵ＫＰｍ７によって、暗号化処理部３１８によって暗号化される（ステップＳ１２２）。

【０２０９】トランザクションＩＤおよび暗号化されたセッションキーＫｓ１は、トランザクションＩＤ／／｛Ｋｓ１｝Ｋｍ７として、バスＢＳ１および通信装置３５０を介して外部に出力される（ステップＳ１２４）。

【０２１０】図１４を参照して、パーソナルコンピュータ５０が、トランザクションＩＤ／／｛Ｋｓ１｝Ｋｍ７を受信すると（ステップＳ１２６）、コントローラ５１０は、トランザクションＩＤ／／｛Ｋｓ１｝Ｋｍ７をライセンス管理デバイス５２０に入力する（ステップＳ１２８）。そうすると、ライセンス管理デバイス５２０においては、端子５２２６およびインタフェース５２２４を介して、バスＢＳ５に与えられた受信データを、復号処理部５２２２が、保持部５２２１に保持されるライセンス管理デバイス５２０にクラス秘密復号鍵Ｋｍ７によりて復号処理することにより、セッションキーＫｓ１を復号し、セッションキーＫｓ１を受理する（ステップＳ１３０）。

【０２１１】コントローラ５２２０は、配信サーバ１０で生成されたセッションキーＫｓ１の受理を確認すると、セッションキー発生部５２１８に対してライセンス管理デバイス５２０において配信動作時に生成されるセッションキーＫｓ２の生成を指示する。そして、セッションキー発生部５２１８は、セッションキーＫｓ２を生成する（ステップＳ１３２）。

【０２１２】また、配信セッションにおいては、コントローラ５２２０は、ライセンス管理デバイス５２０内のメモリ５２１５に記録されている禁止クラスリストＣＲＬから更新日時ＣＲＬｄａｔｅをメモリ１４１５から抽出して切換スイッチ５２４６に出力する（ステップＳ１３４）。

【０２１３】暗号化処理部５２０６は、切換スイッチ５２４２の接点Ｐａを介して復号処理部５２２２より与えられるセッションキーＫｓ１によって、切換スイッチ５２４６の接点を順次切換えることによって与えられるセッションキーＫｓ２、個別公開暗号鍵ＫＰｍｃ８および禁止クラスリストの更新日時ＣＲＬｄａｔｅを１つのデータ列として暗号化して、｛Ｋｓ２／／ＫＰｍｃ８／／ＣＲＬｄａｔｅ｝Ｋｓ１をバスＢＳ３に出力する（ステップＳ１３６）。

【０２１４】バスＢＳ３に出力された暗号化データ｛Ｋｓ２／／ＫＰｍｃ８／／ＣＲＬｄａｔｅ｝Ｋｓ１は、バスＢＳ３からインタフェース５２２４および端子５２２６を介してパーソナルコンピュータ５０に出力され、パーソナルコンピュータ５０から配信サーバ１０に送信される（ステップＳ１３８）。

【０２１５】配信サーバ１０は、トランザクションＩＤ／／｛Ｋｓ２／／ＫＰｍｃ８／／ＣＲＬｄａｔｅ｝Ｋｓ１を受信して、復号処理部３２０においてセッションキーＫｓ１による復号処理を実行し、ライセンス管理デバイス５２０で生成されたセッションキーＫｓ２、ライセンス管理デバイス５２０固有の個別公開暗号鍵ＫＰｍｃ８およびライセンス管理デバイス５２０における禁止クラスリストの更新日時ＣＲＬｄａｔｅを受理する（ステ

ップＳ１４２）。

【０２１６】配信制御部３１５は、ステップＳ１１０で取得したコンテンツＩＤおよびライセンス購入条件ＡＣに従って、アクセス制限情報ＡＣｍおよび再生期限ＡＣｐを生成する（ステップＳ１４４）。さらに、暗号化コンテンツデータを復号するためのライセンス鍵Ｋｃを情報データベース３０４より取得する（ステップＳ１４６）。

【０２１７】配信制御部３１５は、生成したライセンス、すなわち、トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、再生期限ＡＣｐ、およびアクセス制限情報ＡＣｍを暗号化処理部３２６に与える。暗号化処理部３２６は、復号処理部３２０によって得られたライセンス管理デバイス５２０固有の個別公開暗号鍵ＫＰｍｃ８によってライセンスを暗号化して暗号化データ｛トランザクションＩＤ//コンテンツＩＤ//Ｋｃ//ＡＣｍ//ＡＣｐ｝Ｋｍｃ８を生成する（ステップＳ１４８）。

【０２１８】図１５を参照して、配信サーバ１０において、ライセンス管理デバイス５２０から送信された禁止クラスリストの更新日時ＣＲＬｄａｔｅを、ＣＲＬデータベース３０６に保持される配信サーバ１０の禁止クラスリストＣＲＬの更新日時と比較することによって、ライセンス管理デバイス５２０は保持する禁止クラスリストＣＲＬが最新か否かが判断され、最新と判断されたとき、ステップＳ１５２へ移行する。また、最新でないときはステップＳ１６０へ移行する（ステップＳ１５０）。

【０２１９】最新と判断されたとき、暗号化処理部３２８は、暗号化処理部３２６から出力された暗号化データ｛トランザクションＩＤ//コンテンツＩＤ//Ｋｃ//ＡＣｍ//ＡＣｐ｝Ｋｍｃ８をライセンス管理デバイス５２０において発生されたセッションキーＫｓ２によって暗号化を行い、暗号化データ｛｛トランザクションＩＤ//コンテンツＩＤ//Ｋｃ//ＡＣｍ//ＡＣｐ｝Ｋｍｃ８｝Ｋｓ２をバスＢＳ１に出力する。そして、配信制御部３１５は、バスＢＳ１上の暗号化データ｛｛トランザクションＩＤ//コンテンツＩＤ//Ｋｃ//ＡＣｍ//ＡＣｐ｝Ｋｍｃ８｝Ｋｓ２を通信装置３５０を介してパーソナルコンピュータ５０へ送信する（ステップＳ１５２）。

【０２２０】そして、パーソナルコンピュータ５０のコントローラ５１０は、暗号化データ｛｛トランザクションＩＤ//コンテンツＩＤ//Ｋｃ//ＡＣｍ//ＡＣｐ｝Ｋｍｃ８｝Ｋｓ２を受信し（ステップＳ１５４）、バスＢＳ５を介してライセンス管理デバイス５２０に入力する。ライセンス管理デバイス５２０の復号処理部５２１２は、暗号化データ｛｛トランザクションＩＤ//コンテンツＩＤ//Ｋｃ//ＡＣｍ//ＡＣｐ｝Ｋｍｃ８｝Ｋｓ２を端子５２２６およびインタフェース５２２４を介して受取り、セッションキー発生部５２１８によって発生されたセッションキーＫｓ２によって復号し、｛トランザクションＩＤ//コンテンツＩＤ//Ｋｃ//ＡＣｍ//ＡＣｐ｝Ｋｍｃ８を受理する（ステップＳ１５８）。その後、ステップＳ１７２へ移行する。

【０２２１】一方、最新でないと判断されると、配信制御部３１５は、バスＢＳ１を介してＣＲＬデータベース３０６から最新の禁止クラスリストＣＲＬを取得し、差分データである差分ＣＲＬを生成する（ステップＳ１６０）。

【０２２２】暗号化処理部３２８は、暗号化処理部３２６の出力と、配信制御部３１５がバスＢＳ１を介して供給する禁止クラスリストの差分ＣＲＬとを受けて、ライセンス管理デバイス５２０において生成されたセッションキーＫｓ２によって暗号化する。暗号化処理部３２８より出力された暗号化データ｛差分ＣＲＬ//｛トランザクションＩＤ//コンテンツＩＤ//Ｋｃ//ＡＣｍ//ＡＣｐ｝Ｋｍｃ８｝Ｋｓ２は、バスＢＳ１および通信装置３５０を介してパーソナルコンピュータ５０に送信される（ステップＳ１６２）。

【０２２３】パーソナルコンピュータ５０は、送信された暗号化データ｛差分ＣＲＬ//｛トランザクションＩＤ//コンテンツＩＤ//Ｋｃ//ＡＣｍ//ＡＣｐ｝Ｋｍｃ８｝Ｋｓ２を受信し（ステップＳ１６４）、バスＢＳ５を介してライセンス管理デバイス５２０に入力する（ステップＳ１６６）。ライセンス管理デバイス５２０においては、端子５２２６およびインタフェース５２２４を介して、バスＢＳ５に与えられた受信データを復号処理部５２１２によって復号する。復号処理部５２１２は、セッションキー発生部５２１８から与えられたセッションキーＫｓ２を用いてバスＢＳ５の受信データを復号しバスＢＳ５に出力する（ステップＳ１６８）。

【０２２４】この段階で、バスＢＳ５には、Ｋｍｃ保持部５２２１に保持される秘密復号鍵Ｋｍｃ８で復号可能な暗号化ライセンス｛トランザクションＩＤ//コンテンツＩＤ//Ｋｃ//ＡＣｍ//ＡＣｐ｝Ｋｍｃ８｝と、差分ＣＲＬとが出力される（ステップＳ１６８）。コントローラ５２２０の指示によって受理した差分ＣＲＬによってメモリ５２１５内のＣＲＬ領域５２１５Ａを差分ＣＲＬに基づいて更新する（ステップＳ１７０）。

【０２２５】ステップＳ１５２，Ｓ１５４，Ｓ１５６，Ｓ１５８は、ライセンス管理デバイス５２０が保持する禁止クラスリストＣＲＬが最新の場合のライセンス鍵Ｋｃ等のライセンス管理デバイス５２０への配信動作であり、ステップＳ１６０，Ｓ１６２，Ｓ１６４，Ｓ１６６，Ｓ１６８，Ｓ１７０は、ライセンス管理デバイス５２０が保持する禁止クラスリストＣＲＬが最新でない場合のライセンス鍵Ｋｃ等のライセンス管理デバイス５２０への配信動作である。このように、ライセンス管理デバイス５２０から送られてきた禁止クラスリストの更新

日時ＣＲＬｄａｔｅが最新の更新日時か否かを、逐一、確認し、最新でないとき、最新の禁止クラスリストＣＲＬｄａｔｅをＣＲＬデータベース３０６から取得し、差分ＣＲＬをライセンス管理デバイス５２０に配信することによって、ライセンスの破られたライセンス管理デバイスへの配信したライセンスの流出を防止できる。

【０２２６】ステップＳ１５８またはステップＳ１７０の後、コントローラ５２２０の指示によって、暗号化ライセンス〔トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ〕Ｋｍｃ８は、復号処理部５２０４において、個別秘密復号鍵Ｋｍｃ８によって復号され、ライセンス（ライセンス鍵Ｋｃ、トランザクションＩＤ、コンテンツＩＤ、アクセス制限情報ＡＣｍおよび再生期限ＡＣｐ）が受理される（ステップＳ１７２）。

【０２２７】図１６を参照して、コントローラ５１０は、ライセンス管理デバイス５２０が受理したライセンスを格納するエントリを指示するためのエントリ番号を、ライセンス管理デバイス５２０に入力する（ステップＳ１７４）。そうすると、ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６およびインタフェース５２２４を介してエントリ番号を受取り、その受取ったエントリ番号によって指定されるメモリ５２１５のライセンス領域５２１５Ｂに、ステップＳ１７２において取得したライセンス（ライセンス鍵Ｋｃ、トランザクションＩＤ、コンテンツＩＤ、アクセス制限情報ＡＣｍおよび再生期限ＡＣｐ）を格納する（ステップＳ１７６）。

【０２２８】パーソナルコンピュータ５０のコントローラ５１０は、配信サーバ１０から送られたトランザクションＩＤと、暗号化コンテンツデータの配信要求を配信サーバ１０へ送信する（ステップＳ１７８）。

【０２２９】配信サーバ１０は、トランザクションＩＤおよび暗号化コンテンツデータの配信要求を受信し（ステップＳ１８０）、情報データベース３０４より、暗号化コンテンツデータ〔Ｄｃ〕Ｋｃおよび付加情報Ｄｃ－ｉｎｆを取得して、これらのデータをバスＢＳ１および通信装置３５０を介して出力する（ステップＳ１８２）。

【０２３０】パーソナルコンピュータ５０は、〔Ｄｃ〕Ｋｃ／／Ｄｃ－ｉｎｆを受信して、暗号化コンテンツデータ〔Ｄｃ〕Ｋｃおよび付加情報Ｄｃ－ｉｎｆを受理する（ステップＳ１８４）。そうすると、コントローラ５１０は、暗号化コンテンツデータ〔Ｄｃ〕Ｋｃおよび付加情報Ｄｃ－ｉｎｆを１つのコンテンツファイルとしてバスＢＳ２を介してハードディスク（ＨＤＤ）５３０に記録する（ステップＳ１８６）。また、コントローラ５１０は、ライセンス管理デバイス５２０に格納されたライセンスのエントリ番号と、平文のトランザクションＩＤおよびコンテンツＩＤを含む暗号化コンテンツデータ〔Ｄｃ〕Ｋｃと付加情報Ｄｃ－ｉｎｆに対するライセンス管理ファイルを生成し、バスＢＳ２を介してＨＤＤ５３０に記録する（ステップＳ１８８）。さらに、コントローラ５１０は、ＨＤＤ５３０に記録されているコンテンツリストファイルに受理したコンテンツの情報として、記録したコンテンツファイル及びライセンス管理ファイルの名称や、付加情報Ｄｃ－ｉｎｆから抽出した暗号化コンテンツデータに関する情報（曲名、アーティスト名）等を追記し（ステップＳ１９０）、トランザクションＩＤと配信要求を配信サーバ１０へ送信する（ステップＳ１９２）。

【０２３１】配信サーバ１０は、トランザクションＩＤ／／配信要求を受信すると（ステップＳ１９４）、課金データベース３０２への課金データの格納、およびトランザクションＩＤの配信記録データベース３０８への記録が行われて配信終了の処理が実行され（ステップＳ１９６）、全体の処理が終了する（ステップＳ１９８）。

【０２３２】このようにして、パーソナルコンピュータ５０に内蔵されたライセンス管理デバイス５０が正規の認証データを保持する機器であること、同時に、クラス証明書Ｃｍ７とともに暗号化して送信できた公開暗号鍵ＫＰｍ７が有効であることを確認した上で、クラス証明書Ｃｍ７が禁止クラスリスト、すなわち、公開暗号鍵ＫＰｍ７による暗号化が破られたクラス証明書リストに記載されていないライセンス管理デバイスからの配信要求に対してのみコンテンツデータを配信することができ、不正なライセンス管理デバイスへの配信および解読されたクラス鍵を用いた配信を禁止することができる。

【０２３３】また、配信サーバおよびライセンス管理デバイスでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

【０２３４】また、ライセンス管理デバイス５２０は、配信サーバ１０から暗号化コンテンツデータおよびライセンスを受信する際に、配信サーバ１０との間でハード的にデータのやり取りを行ない、暗号化コンテンツデータを再生するためのライセンスをハード的に格納するため、そのセキュリティレベルは高い。したがって、ライセンス管理デバイス５２０を用いれば、パーソナルコンピュータ５０は、セキュリティレベルの高い配信によって暗号化コンテンツデータおよびライセンスを受信できるとともに、セキュリティレベルの高いレベル２ライセンスの管理が可能である。

【０２３５】〔配信２〕図１に示すデータ配信システムにおいて、配信サーバ１０からパーソナルコンピュータ５０のライセンス管理モジュール５１１へ暗号化コンテンツデータおよびライセンスを配信する動作について説

明する。なお、この動作を「配信２」という。

【０２３６】図１７～図２１は、図１に示すデータ配信システムにおける暗号化コンテンツデータの購入時に発生するパーソナルコンピュータ５０に内蔵されたライセンス管理モジュール５１１への配信動作を説明するための第１～第５のフローチャートである。なお、ライセンス管理モジュール５１１は、暗号化コンテンツデータおよびライセンスの配信サーバ１０からの受信をプログラムによって実行する。

【０２３７】図１７における処理以前に、パーソナルコンピュータ５０のユーザは、配信サーバ１０に対してモデム４０を介して接続し、購入を希望するコンテンツに対するコンテンツＩＤを取得していることを前提としている。

【０２３８】図１７を参照して、パーソナルコンピュータ５０のユーザからキーボード５６０を介してコンテンツＩＤの指定による配信リクエストがなされる（ステップＳ２００）。そして、キーボード５６０を介して暗号化コンテンツデータのライセンスを購入するための購入条件ＡＣが入力される（ステップＳ２０２）。つまり、選択した暗号化コンテンツデータを復号するライセンス鍵Ｋｃを購入するために、暗号化コンテンツデータのアクセス制限情報ＡＣｍ、および再生期限ＡＣｐを設定して購入条件ＡＣが入力される。

【０２３９】暗号化コンテンツデータの購入条件ＡＣが入力されると、コントローラ５１０は、ライセンス管理モジュール５１１から認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰａ２を読出し、その読出した認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰａ２に加えて、コンテンツＩＤ、ライセンス購入条件のデータＡＣ、および配信リクエストを配信サーバ１０に対して送信する（ステップＳ２０４）。

【０２４０】配信サーバ１０では、パーソナルコンピュータ５０から配信リクエスト、コンテンツＩＤ、認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰａ２、およびライセンス購入条件のデータＡＣを受信し（ステップＳ２０６）、復号処理部３１２においてライセンス管理モジュール５１１から出力された認証データをレベル１認証鍵ＫＰａ１で復号処理を実行する（ステップＳ２０８）。

【０２４１】配信制御部３１５は、復号処理部３１２における復号処理結果から、処理が正常に行なわれたか否か、すなわち、正規の機関でクラス公開暗号鍵ＫＰｍ５とクラス証明書Ｃｍ５の正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ２１０）。正当な認証データであると判断された場合、配信制御部３１５は、クラス公開暗号鍵ＫＰｍ５およびクラス証明書Ｃｍ５を承認し、受理する。そして、次の処理（ステップＳ２１２）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵ＫＰｍ５およびクラス証明書Ｃｍ５を受理しないで処理を終了する（ステップＳ２８８）。

【０２４２】認証の結果、正規のモジュールであることが認識されると、配信制御部３１５は、次に、ライセンス管理モジュール５１１のクラス証明書Ｃｍ５が禁止クラスリストＣＲＬにリストアップされているかどうかをＣＲＬデータベース３０６に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する（ステップＳ２８８）。

【０２４３】一方、ライセンス管理モジュール５１１のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップＳ２１４）。

【０２４４】認証の結果、正当な認証データを持つライセンス管理モジュールを備えるパーソナルコンピュータからのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、配信サーバ１０においても、配信制御部３１５は、配信を特定するための管理コードであるトランザクションＩＤを生成する（ステップＳ２１４）。また、セッションキー発生部３１６は、配信のためのセッションキーＫｓ１を生成する（ステップＳ２１６）。セッションキーＫｓ１は、復号処理部３１２によって得られたライセンス管理モジュール５１１に対応するクラス公開暗号鍵ＫＰｍ５によって、暗号化処理部３１８によって暗号化される（ステップＳ２１８）。

【０２４５】トランザクションＩＤおよび暗号化されたセッションキーＫｓ１は、トランザクションＩＤ／／｛Ｋｓ１｝Ｋｍ５として、バスＢＳ１および通信装置３５０を介して外部に出力される（ステップＳ２２０）。

【０２４６】図１８を参照して、パーソナルコンピュータ５０のコントローラ５１０が、トランザクションＩＤ／／｛Ｋｓ１｝Ｋｍ５を受信すると（ステップＳ２２２）、ライセンス管理モジュール５１１は、｛Ｋｓ１｝Ｋｍ５を受けて、ライセンス管理モジュール５１１に固有のクラス秘密復号鍵Ｋｍ５により復号処理して、セッションキーＫｓ１を受理する（ステップＳ２２４）。

【０２４７】ライセンス管理モジュール５１１は、配信サーバ１０で生成されたセッションキーＫｓ１の受理を確認すると、セッションキーＫｓ２を生成する（ステップＳ２２６）。そして、コントローラ５１０は、バスＢＳ２を介してＨＤＤ５３０に記憶された暗号化ＣＲＬを読出し、ライセンス管理モジュール５１１は、暗号化ＣＲＬを復号して禁止クラスリストＣＲＬを取得し、復号した禁止クラスリストＣＲＬに基づいて禁止クラスリストの更新日時ＣＲＬｄａｔｅを取得する（ステップＳ２２８）。ライセンス管理モジュール５１１は、さらに、配信サーバ１０において発生されたセッションキーＫｓ１によって、ライセンス管理モジュール５１１で発生させたセッションキーＫｓ２、個別公開暗号鍵ＫＰｍｃ６および禁止クラスリストのデータＣＲＬｄａｔｅを１つ

のデータ列として暗号化して、｛Ｋｓ２／／ＫＰｍｃ６／／ＣＲＬｄａｔｅ｝Ｋｓ１を出力する（ステップＳ２３０）。

【０２４８】コントローラ５１０は、暗号化データ｛Ｋｓ２／／ＫＰｍｃ６／／ＣＲＬｄａｔｅ｝Ｋｓ１にトランザクションＩＤを加えたトランザクションＩＤ／／｛Ｋｓ２／／ＫＰｍｃ６／／ＣＲＬｄａｔｅ｝Ｋｓ１を配信サーバ１０へ送信する（ステップＳ２３２）。

【０２４９】配信サーバ１０は、トランザクションＩＤ／／｛Ｋｓ２／／ＫＰｍｃ６／／ＣＲＬｄａｔｅ｝Ｋｓ１を受信して（ステップＳ２３４）、復号処理部３２０においてセッションキーＫｓ１による復号処理を実行し、ライセンス管理モジュール５１１で生成されたセッションキーＫｓ２、ライセンス管理モジュール５１１に固有の個別公開暗号鍵ＫＰｍｃ６およびライセンス管理モジュール５１１における禁止クラスリストの更新日時ＣＲＬｄａｔｅを受理する（ステップＳ２３６）。

【０２５０】配信制御部３１５は、ステップＳ２０６で取得したコンテンツＩＤおよびライセンス購入条件のデータＡＣに従って、アクセス制限情報ＡＣｍおよび再生期限ＡＣｐを生成する（ステップＳ２３８）。さらに、暗号化コンテンツデータを復号するためのライセンス鍵Ｋｃを情報データベース３０４より取得する（ステップＳ２４０）。

【０２５１】配信制御部３１５は、生成したライセンス、すなわち、トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、再生期限ＡＣｐ、およびアクセス制限情報ＡＣｍを暗号化処理部３２６に与える。暗号化処理部３２６は、復号処理部３２０によって得られたライセンス管理モジュール５１１に固有の個別公開暗号鍵ＫＰｍｃ６によってライセンスを暗号化して暗号化データ｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６を生成する（ステップＳ２４２）。

【０２５２】図１９を参照して、配信サーバ１０において、ライセンス管理モジュール５１１から送信された禁止クラスリストの更新日時ＣＲＬｄａｔｅによって、配信を求めてきたライセンス管理デバイス５２０の禁止クラスリストＣＲＬが最新か否かが判断され、ライセンス管理モジュールの禁止クラスリストＣＲＬが最新と判断されたとき、ステップＳ２４６へ移行する。また、最新でないと判断されたときはステップＳ２５２へ移行する（ステップＳ２４４）。

【０２５３】最新と判断されたとき、暗号化処理部３２８は、暗号化処理部３２６から出力された暗号化データ｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６をライセンス管理モジュール５１１において発生されたセッションキーＫｓ２によって暗号化を行い、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６｝Ｋｓ２をパスＢＳ１に出力する。そして、配信制御部３１５は、パスＢＳ１上の暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６｝Ｋｓ２を通信装置３５０を介してパーソナルコンピュータ５０へ送信する（ステップＳ２４６）。

【０２５４】そして、パーソナルコンピュータ５０のコントローラ５１０は、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６｝Ｋｓ２を受信し（ステップＳ２４８）、ライセンス管理モジュール５１１は、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６｝Ｋｓ２をセッションキーＫｓ２によって復号し、｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６を受理する（ステップＳ２５０）。その後、ステップＳ２６２へ移行する。

【０２５５】一方、最新でないと判断されると、配信制御部３１５は、パスＢＳ１を介してＣＲＬデータベース３０６から最新の禁止クラスリストＣＲＬを取得し、差分データである差分ＣＲＬを生成する（ステップＳ２５２）。

【０２５６】暗号化処理部３２８は、暗号化処理部３２６の出力と、配信制御部３１５がパスＢＳ１を介して供給する禁止クラスリストの差分ＣＲＬとを受けて、ライセンス管理モジュール５１１において生成されたセッションキーＫｓ２によって暗号化する。暗号化処理部３２８より出力された暗号化データ｛差分ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６｝Ｋｓ２は、パスＢＳ１および通信装置３５０を介してパーソナルコンピュータ５０に送信される（ステップＳ２５４）。

【０２５７】パーソナルコンピュータ５０は、送信された暗号化データ｛差分ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６｝Ｋｓ２を受信し（ステップＳ２５６）、ライセンス管理モジュール５１１は、セッションキーＫｓ２を用いて受信データを復号して差分ＣＲＬと暗号化データ｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６と受理する（ステップＳ２５８）。

【０２５８】コントローラ５１０は、ＨＤＤ５３０に記録された禁止クラスリストＣＲＬに受理した差分ＣＲＬを加え、独自の暗号処理を施し、ＨＤＤ５３０内の禁止クラスリストＣＲＬを書換える（ステップＳ２６０）。

【０２５９】ステップＳ２４６，Ｓ２４８，Ｓ２５０は、ライセンス管理モジュール５１１から送られてきた禁止クラスリストの更新日時ＣＲＬｄａｔｅによって、ライセンス管理モジュール５１１の管理する禁止クラスリストＣＲＬが最新の場合のライセンスのライセンス管

理モジュール５１１への配信動作であり、ステップＳ２５２，Ｓ２５４，Ｓ２５６，Ｓ２５８，Ｓ２６０は、禁止クラスリストＣＲＬが最新でない場合のライセンスのライセンス管理モジュール５１１への配信動作である。このように、ライセンス管理モジュール５１１から送られてきた禁止クラスリストの更新日時ＣＲＬｄａｔｅによって、配信を求めてきたライセンス管理デバイス５２０の禁止クラスリストＣＲＬが最新か否かを、逐一、確認し、最新でないとき、最新の禁止クラスリストＣＲＬをＣＲＬデータベース３０６から取得し、差分ＣＲＬをライセンス管理モジュール５１１に配信することによって、ライセンス管理モジュールへ配信したライセンスがセキュリティの破られた機器へ流出されるのを防止できる。

【０２６０】ステップＳ２５０またはステップＳ２６０の後、暗号化テキスト｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６は、個別秘密復号鍵Ｋｍｃ６によって復号され、ライセンス（ライセンス鍵Ｋｃ、トランザクションＩＤ、コンテンツＩＤ、アクセス制限情報ＡＣｍおよび再生期限ＡＣｐ）が受理される（ステップＳ２６２）。

【０２６１】このように、配信サーバおよびライセンス管理モジュールでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

【０２６２】ライセンス管理モジュール５１１は、受理したアクセス制限情報ＡＣｍによって再生回数が制限されているか否かを判別し、再生回数が制限されていないときステップＳ２６６へ移行し、再生回数が制限されているときステップＳ２６８へ移行する（ステップＳ２６４）。そして、再生回数が制限されていなとき、ライセンス管理モジュール５１１は、配信サーバ１０から受信した暗号化コンテンツおよびライセンスを他の装置へ貸出すためのチェックアウト可能数を含むチェックアウト情報を生成する（ステップＳ２６６）。この場合、チェックアウトの初期値は「３」に設定される。また、再生回数が制限されているとき、ライセンス管理モジュール５１１は、暗号化コンテンツデータを他の装置へ貸出すためのチェックアウト可能数を「０」に設定してチェックアウト情報を生成する（ステップＳ２６８）。ステップＳ２６８は、チェックアウトすることで再生回数の管理ができないための処理である。

【０２６３】図２０を参照して、ステップＳ２６６またはステップＳ２６８の後、ライセンス管理モジュール５１１は、認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰａ１をパス２を介してライセンス管理デバイス５２０へ出力する（ステップＳ２７０）。ライセンス管理デバイス５２０では、ライセンス管理モジュール５１１から認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰａ１を受信し、復号処理部５２０８は、認証データ認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰａ１を受取って、認証データ認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰａ１に基づいて、ＫＰａ保持部５２１４からレベル１認証鍵ＫＰａ１を受取り、受取ったレベル１認証鍵ＫＰａ１によって認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰａ１を復号する（ステップＳ２７１）。

【０２６４】コントローラ５２２０は、復号処理部５２０８における復号処理結果から、処理が正常に行なわれたか否か、すなわち、正規の機関でクラス公開暗号鍵ＫＰｍ５とクラス証明書Ｃｍ５との正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ２７２）。正当な認証データであると判断された場合、コントローラ５２２０は、クラス公開暗号鍵ＫＰｍ５およびクラス証明書Ｃｍ５を承認し、受理する。そして、次の処理（ステップＳ２７３）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵ＫＰｍ５およびクラス証明書Ｃｍ５を受理しないで処理を終了する（ステップＳ２９８）。

【０２６５】認証の結果、正規の認証データを受信したことが認識されると、コントローラ５２２０は、次に、ライセンス管理モジュール５１１のクラス証明書Ｃｍ５が禁止クラスリストＣＲＬにリストアップされているかどうかをメモリ５２１５のＣＲＬ領域５２１５Ａに照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する（ステップＳ２９８）。

【０２６６】一方、ライセンス管理モジュール５１１のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップＳ２７３）。

【０２６７】認証の結果、正当な認証データを持つライセンス管理デバイスを備えるライセンス管理モジュール５１１からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、ライセンス管理デバイス５２０において、セッションキー発生部５２０８は、セッションキーＫｓ２ａを生成し（ステップＳ２７４）、暗号処理部５２１０は、セッションキーＫｓ２ａをクラス公開暗号鍵ＫＰｍ５によって暗号化して暗号化データ｛Ｋｓ２ａ｝Ｋｍ５を出力する（ステップＳ２７５）。

【０２６８】コントローラ５２２０は、暗号化データ｛Ｋｓ２ａ｝Ｋｍ５をバスＢＳ５、インタフェース５２２４、および端子５２２６を介して出力し、ライセンス管理モジュール５１１は、バスＢＳ２を介して暗号化データ｛Ｋｓ２ａ｝Ｋｍ５を受信し、クラス秘密復号鍵Ｋｍ５によって暗号化データ｛Ｋｓ２ａ｝Ｋｍ５を復号してセッションキーＫｓ２ａを受理する（ステップＳ２７

６）。そして、ライセンス管理モジュール５１１は、セッションキーＫｓ２ｂを生成し（ステップＳ２７７）、セッションキーＫｓ２ｂをセッションキーＫｓ２ａによって暗号化して暗号化データ｛Ｋｓ２ｂ｝Ｋｓ２ａをバスＢＳ２を介してライセンス管理デバイス５２０へ出力する（ステップＳ２７８）。

【０２６９】ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６、インタフェース５２２４、およびバスＢＳ５を介して暗号化データ｛Ｋｓ２ｂ｝Ｋｓ２ａを受け、復号処理部５２１２は、セッションキー発生部５２０８から出力されるセッションキーＫｓ２ａによって暗号化データ｛Ｋｓ２ｂ｝Ｋｓ２ａを復号してセッションキーＫｓ２ｂを受理する（ステップＳ２７９）。そうすると、ライセンス管理モジュール５１１は、エントリ番号「０」をライセンス管理デバイス５２０へ入力し（ステップＳ２８０）、ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６、インタフェース５２２４、およびバスＢＳ５を介してエントリ番号「０」を受取る。そして、コントローラ５２２０は、メモリ５２１５のライセンス領域５２１５Ｂのうち、エントリ番号「０」によって指定されている領域に格納されているバインディングライセンス（トランザクションＩＤｂ、コンテンツＩＤｂ、バインディング鍵Ｋｂ、および制御情報ＡＣｍｂ，ＡＣｐｂ）を取得する（ステップＳ２８１）。そして、コントローラ５２２０は、制御情報ＡＣｍｂに基づいてバインディングライセンスが有効か否かを判別し、有効でない場合、ステップＳ２９８へ移行し、配信セッションが終了する。ここで、有効な場合とは、制御情報ＡＣｍｂ内の再生回数が０でないこと、かつ、レベル１認証鍵ＫＰａ１によって認証された処理であるため制御情報ＡＣｍｂのセキュリティレベルがレベル１であることを意味する。

【０２７０】一方、バインディングライセンスが有効な場合、ステップＳ２８３へ移行する（ステップＳ２８２）。

【０２７１】ステップＳ２８２において、バインディングライセンスが有効と判断されると、暗号処理部５２０６は、切換スイッチ５２４６を介して取得したバインディング鍵Ｋｂおよび制御情報ＡＣｐｂを、復号処理部５２１２によって復号され、スイッチ５２４２を介して取得したセッションキーＫｓ２ｂによって暗号化して暗号化データ｛Ｋｂ／／ＡＣｐｂ｝Ｋｓ２ｂを出力する（ステップＳ２８３）。

【０２７２】図２１を参照して、コントローラ５２２０は、暗号化データ｛Ｋｂ／／ＡＣｐｂ｝Ｋｓ２ｂをバスＢＳ５、インタフェース５２２４、および端子５２２６を介して出力し、ライセンス管理モジュール５１１は、バスＢＳ２を介して暗号化データ｛Ｋｂ／／ＡＣｐｂ｝Ｋｓ２ｂを受信し、セッションキーＫｓ２ｂによって暗号化データ｛Ｋｂ／／ＡＣｐｂ｝Ｋｓ２ｂを復号してバインディング鍵Ｋｂおよび制御情報ＡＣｐｂを取得する（ステップＳ２８４）。

【０２７３】ステップＳ２７０からステップＳ２８４の一連の処理はバインディング鍵Ｋｂをライセンス管理デバイス５２０から取得する処理であり、「バインディング鍵取得処理」と総称する。

【０２７４】そして、ライセンス管理モジュール５１１は、バスＢＳ２を介してＨＤＤ５３０から暗号化機密ファイル１６０を取得し、その取得した暗号化機密ファイル１６０をバインディング鍵Ｋｂによって復号して平文の機密ファイルを取得する（ステップＳ２８５）。そうすると、ライセンス管理モジュール５１１は、配信サーバ１０から受理したライセンス（トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍ、および再生期限ＡＣｐ）とステップＳ２６６またはステップＳ２６８において生成されたチャックアウト情報とを機密情報ｎとして平文の機密ファイルに追記する（ステップＳ２８６）。その後、ライセンス管理モジュール５１１は、平文の機密ファイルをバインディング鍵Ｋｂによって再び暗号化し、その暗号化した暗号化機密ファイル１６０によってＨＤＤ５３０に記録された暗号化機密ファイル１６０を更新する（ステップＳ２８７）。ライセンスを暗号化機密ファイル１６０に格納した後、ライセンス管理モジュール５１１は、配信サーバ１０から送られたトランザクションＩＤと、暗号化コンテンツデータの配信要求を配信サーバ１０へ送信する（ステップＳ２８８）。

【０２７５】配信サーバ１０は、トランザクションＩＤおよび暗号化コンテンツデータの配信要求を受信し（ステップＳ２８９）、情報データベース３０４より、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆｏを取得して、これらのデータをバスＢＳ１および通信装置３５０を介して出力する（ステップＳ２９０）。

【０２７６】ライセンス管理モジュール５１１は、｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆｏを受信して、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆｏを受理する（ステップＳ２９１）。そして、ライセンス管理モジュール５１１は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆｏをバスＢＳ２を介してコンテンツファイルとしてハードディスク（ＨＤＤ）５３０に記録する（ステップＳ２９２）。また、ライセンス管理モジュール５１１は、暗号化機密ファイル１６０に格納した機密情報ｎの機密情報番号ｎと、平文のトランザクションＩＤおよびコンテンツＩＤとを含むコンテンツファイル（暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆ）に対応するライセンス管理ファイルを生成し、バスＢＳ２を介してＨＤＤ５３０に記録する（ステップＳ２９３）。さらに、ライセンス管理モジュール５１１は、ＨＤＤ５３０に記録されているコン

テンツリストファイルに受理したコンテンツ情報として、記録したコンテンツファイルおよびライセンス管理ファイルの名称や、付加情報Ｄｅｓｃｒｉｐｔｏｒから抽出した暗号化コンテンツデータに関する情報（曲名、アーティスト名）等を追記し（ステップＳ２９４）、トランザクションＩＤと配信受理を配信サーバ１０へ送信する（ステップＳ２９５）。

【０２７７】配信サーバ１０は、トランザクションＩＤ／／配信受理を受信すると（ステップＳ２９６）、課金データベース３０２への課金データの格納、およびトランザクションＩＤの配信記録データベース３０８への記録が行なわれて配信終了の処理が実行され（ステップＳ２９７）、全体の処理が終了する（ステップＳ２９８）。

【０２７８】このように、ライセンス管理モジュール５１１は、配信サーバ１０との間でバッドウエアによってデータのやり取りを行ない、暗号化コンテンツデータおよびライセンスをソフト的に配信サーバ１０から受信する。また、受信した暗号化コンテンツデータをＨＤＤ５３０に記録し、ライセンスを機密情報ｎとして機密ファイルに書込み、その機密ファイルをバインディング鍵Ｋｂによって暗号化して暗号化機密ファイル１６０にライセンスを格納する。そして、暗号化機密ファイル１６０を復号するバインディング鍵Ｋｂはライセンス管理デバイス５２０に保持される。したがって、ライセンス管理モジュール５１１による暗号化コンテンツデータおよびライセンスの配信は、ライセンス管理デバイス５２０による暗号化コンテンツデータおよびライセンスの配信よりもセキュリティレベルは低いが、記録管理においてはパーソナルコンピュータ５０に関連付けていない点において、それに近いものになる。

【０２７９】［リッピング］パーソナルコンピュータ５０のユーザは配信によって暗号化コンテンツとライセンスを取得するほかに、所有する音楽ＣＤから、音楽データを取得して利用することが可能である。著作権者の権利保護の立場から音楽ＣＤのデジタル複製は自由に行って良いものではないが、個人が自己の使用目的のために、著作権保護機能を備えるツールを用いて複製し、音楽を楽しむことは許されている。そこで、ライセンス管理モジュール５１１は、音楽ＣＤから音楽データを取得して、ライセンス管理モジュール５１１にて管理可能な暗号化コンテンツデータとライセンスを生成するリッピング機能を実現するプログラムも含んでいる。

【０２８０】また、近年の音楽ＣＤには、音楽データ内に、ウォーターマークと呼ばれる電子すかしを挿入したものがある。このウォーターマークには、著作権者が利用者における利用の範囲が利用規則として書込まれている。利用規則が書込まれている音楽データからのリッピングでは、著作権保護の点から必ずこの利用規則に従う必要がある。以後、利用規則として、複製条件（複製禁止／一世代複製可／複製可」および最大チェックアウト数が記載されているとする。また、ウォーターマーク検出されない場合、すなわち、利用規則が書込まれていない従来の音楽ＣＤであっても、著作権者の権利を保護するために、一世代の複製ができ、最大チェックアウト数が「３」と解釈するものとする。

【０２８１】図２２～図２４を参照して、音楽データが記録された音楽ＣＤからのリッピングによる暗号化コンテンツデータおよびライセンスの取得について説明する。

【０２８２】図２２～図２４は、音楽ＣＤからリッピングによって暗号化コンテンツデータおよびライセンスを取得するための第１～第３のフローチャートである。

【０２８３】図２２を参照して、リッピング動作が開始されると、ＣＤ－ＲＯＭドライブ５４０が音楽ＣＤから検出した音楽データを取り込んで、取込んだ音楽データからウォーターマークによって記載された利用規則の検出が行なわれる（ステップＳ７００）。そして、検出された利用規則に基づいて複製が可能か否かが判定される（ステップＳ７０１）。利用規則の複製条件が無制限の場合、ステップＳ２０３へ、複製条件が一世代複製可の場合、ステップＳ７０２へ移行し、複製条件が複製禁止の場合、複製が禁止され、ステップＳ７３３へ移行してリッピング動作は終了する。さらに、装着されたＣＤにウォーターマークが含まれず、利用規則が得られない場合、ステップＳ７０５へ移行する。

【０２８４】ステップＳ７０１において、利用規則の複製条件が一世代複製可の場合、ライセンス管理モジュール５１１は、取得した音楽データに含まれるウォーターマークを取得した利用規則の複製条件を複製禁止に変更したウォーターマークに付け替える（ステップＳ７０２）。そして、ステップＳ７０３へ移行する。複製ができる利用規則が検出された場合にステップＳ７０３において、ライセンス管理モジュール５１１は、利用規則を反映したアクセス制限情報ＡＣｍおよび再生期限ＡＣｐを生成する（ステップＳ７０３）。ここでも、複製条件に従い、複製可であれば、アクセス制限情報ＡＣｍの移動複製フラグを移動複製可（＝３）に設定し、一世代複製可であれば、リッピング自身が一世代に当たるので移動複製禁止（＝０）に設定する。また、対応する利用規則はないが再生回数は無制限、セキュリティレベルはレベル１に設定する。その後、ライセンス管理うモジュール５１１は、利用規則の最大チェックアウト数を反映してチェックアウト可能数を設定する。最大チェックアウト数の指定がないときはチェックアウト可能数＝３とする。そして、設定したチェックアウト可能数を含むチェックアウト情報を生成する（ステップＳ７０４）。

【０２８５】一方、ステップＳ７０１において、ウォーターマークが検出されず、利用規則が無いと判定された場合、ライセンス管理モジュール５１１は、アクセス制

限情報ＡＣｍの移動複製フラグを移動複製禁止（＝０）、再生回数は無制限（＝２５５）、セキュリティレベルは１に設定する。再生期限ＡＣｐは再生を無期限とする（ステップＳ７０５）。その後、ライセンス管理モジュール５１１は、初期値が３であるチェックアウト可能数を含むチェックアウト情報を生成する（ステップＳ７０６）。

【０２８６】ステップＳ７０４またはＳ７０６の後、ライセンス管理モジュール５１１は、乱数などによってライセンス鍵Ｋｃを生成し（ステップＳ７０７）、ローカル使用のトランザクションＩＤおよびコンテンツＩＤを生成する（ステップＳ７０８）。次に、ライセンス管理モジュール５１１は、バインディング鍵取得処理を行う。図２３のステップＳ７０９から図２４のステップ７２３の一連の処理がバインディング鍵取得処理であり、配信２の配信処理における図２０のステップＳ２７０から図２１のステップＳ２８４の一連の処理と同じである。ゆえに、説明を省略する。

【０２８７】図２４を参照して、バインディング鍵Ｋｂを取得したライセンス管理モジュール５１１は、バスＢＳ２を介してＨＤＤ５３０から暗号化機密ファイル１６０を取得し、その取得した暗号化機密ファイル１６０をバインディング鍵Ｋｂによって復号して平文の機密ファイルを取得する（ステップＳ７２４）。そうすると、ライセンス管理モジュール５１１は、音楽ＣＤから取得した音楽データを所定の方式に符号化してコンテンツデータＤｃを生成し（ステップＳ７２５）、コンテンツデータをライセンス鍵Ｋｃによって暗号化して暗号化コンテンツデータ〔Ｄｃ〕Ｋｃを生成する（ステップＳ７２６）。その後、ライセンス管理モジュール５１１は、キーボード５６０を介して入力されたユーザからの情報、および音楽ＣＤからの情報に基づいて、コンテンツデータの付加情報Ｄｃ－ｉｎｆを生成し（ステップＳ７２７）、暗号化コンテンツデータ〔Ｄｃ〕Ｋｃと付加情報Ｄｃ－ｉｎｆとをバスＢＳ２を介してコンテンツファイルとしてＨＤＤ５３０に記録する（ステップＳ７２８）。

【０２８８】そうすると、ライセンス管理モジュール５１１は、生成したライセンス（トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍ、および再生期限ＡＣｐ）とステップＳ７０４またはステップＳ７０６において生成されたチェックアウト情報とを機密情報ｎとして平文の機密ファイルに追記する（ステップＳ７２９）。その後、ライセンス管理モジュール５１１は、平文の機密ファイルをバインディング鍵Ｋｂによって暗号化し、その暗号化した暗号化機密ファイル１６０によってＨＤＤ５３０に記録された暗号化機密ファイル１６０を更新する（ステップＳ７３０）。ライセンスを暗号化機密ファイル１６０に格納した後、ライセンス管理モジュール５１１は、暗号化機密ファイル１６０に格納した機密情報ｎの機密情報番号ｎと、平文のトランザクションＩＤおよびコンテンツＩＤとを含むコンテンツファイル（暗号化コンテンツデータ〔Ｄｃ〕Ｋｃと付加情報Ｄｃ－ｉｎｆ）に対するライセンス管理ファイルを生成し、バスＢＳ２を介してＨＤＤ５３０に記録する（ステップＳ７３１）。さらに、ライセンス管理モジュール５１１は、ＨＤＤ５３０に記録されているコンテンツリストファイルに受理したコンテンツの情報として、記録したコンテンツファイル及びライセンス管理ファイルの名称や、付加情報Ｄｃ－ｉｎｆから抽出した暗号化コンテンツデータに関する情報（曲名、アーティスト名）等を追記し（ステップＳ７３２）、全体の処理が終了する（ステップＳ７３３）。

【０２８９】このように音楽ＣＤからリッピングによっても暗号化コンテンツデータとライセンスとを取得できる。そして、音楽ＣＤからのリッピングによって取得された暗号化コンテンツデータおよびライセンスは、配信によって取得された暗号化コンテンツデータおよびレベル１ライセンスと同じ方式によって、ライセンス管理モジュール５１１によって管理される。

【０２９０】図２５を参照して、パーソナルコンピュータ５０のライセンス管理モジュール５１１またはライセンス管理デバイス５２０によって受信された暗号化コンテンツデータおよびライセンスの管理について説明する。パーソナルコンピュータ５０のＨＤＤ５３０は、コンテンツリストファイル１５０と、コンテンツリストファイル１５０は、コンテンツファイル１５３１～１５３ｎと、ライセンス管理ファイル１５２１～１５２ｎと、暗号化機密ファイルとを含む。

【０２９１】コンテンツリストファイル１５０は、所有するコンテンツの一覧形式のデータファイルであり、個々のコンテンツに対する情報（楽曲名、アーティスト名など）と、コンテンツファイルとライセンス管理ファイルを示す情報（ファイル名）などが含まれている。個々のコンテンツに対する情報は受信時に付加情報Ｄｃ－ｉｎｆから必要な情報を取得して自動的に、あるいは、ユーザの指示によって記載される。また、コンテンツファイルのみ、ライセンス管理ファイルのみの再生できないコンテンツについても一覧の中で管理することが可能である。

【０２９２】コンテンツファイル１５３１～１５３ｎは、ライセンス管理モジュール５１１またはライセンス管理デバイス５２０によって受信された暗号化コンテンツデータ〔Ｄｃ〕Ｋｃと付加情報Ｄｃ－ｉｎｆとを記録するファイルであり、コンテンツごとに設けられる。

【０２９３】また、ライセンス管理ファイル１５２１～１５２ｎは、それぞれ、コンテンツファイル１５３１～１５３ｎに対応して記録されており、ライセンス管理モジュール５１１またはライセンス管理デバイス５２０によって受信されたライセンスを管理するためのファイルであり、ライセンスの格納場所を特定するための情報と

ライセンスに関する情報を含む。

【０２９４】格納場所を特定するための情報とは、ライセンス管理デバイス５２０にライセンスが記録された場合にはエントリ番号、もしくは暗号化機密ファイル内に記録された機密情報を特定する機密情報番号を言う。

【０２９５】ライセンスに関する情報とは、ライセンスを受信したときに平文にて参照できるトランザクションＩＤ、コンテンツＩＤや、ライセンス購入条件ＡＣから容易に判断できるアクセス制限情報ＡＣｍおよび再生制御情報ＡＣｐにて制限されている事項の平文の写しである。これまで説明でも明らかなように、ライセンスは、コンテンツ保護のために参照することができないように保護され、記録されている。しかし、ライセンス鍵Ｋｃを除く他の情報は、書き換えることさえできなければ、その内容が参照されてもコンテンツ保護の立場から何ら問題はない。アプリケーションプログラムにおいて、このライセンスに関する情報を参照して各処理を開始する。

【０２９６】暗号化機密情報ファイルは、ライセンス管理モジュール５１１にて管理されているライセンスやチェックアウト情報などを含む機密情報を含む。暗号化機密情報ファイルは、バインディング鍵Ｋｂにて暗号化されている。

【０２９７】図２５を参照して、具体的に説明する。ライセンス管理ファイル１５２１，１５２４は、それぞれ、エントリ番号１，ｍを含む。これは、ライセンス管理デバイス５２０によって受信され、ライセンス管理デバイス５２０のメモリ５２１５のライセンス領域５２１５Ｂにおいて管理されるライセンス（ライセンスＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍおよび再生期限ＡＣｍ）の管理領域を指定する番号である。

【０２９８】したがって、コンテンツファイル１５３１に記録されたファイル名の暗号化コンテンツデータを再生端末１００に装着されたメモリカード１１０へ移動させるとき、コンテンツファイル１５３１～１５３ｎを検索してコンテンツファイル１５３１を抽出すれば、暗号化コンテンツデータを再生するライセンスがどこで管理されているかが解かる。コンテンツファイル１５３１に対応するライセンス管理ファイル１５２１に含まれるエントリ番号は「１」であるので、コンテンツファイル１５３１に記録されたファイル名の暗号化コンテンツデータを再生するライセンスは、ライセンス管理デバイス５２０のメモリ５２１５のライセンス領域５２１５Ｂのエントリ番号１によって指定された領域に記録されている。そうすると、ＨＤＤ５３０に記録されたコンテンツリストファイル１５０のライセンス管理ファイル１５２１からエントリ番号１を読出し、その読出したエントリ番号１をライセンス管理デバイス５２０に入力することによって、メモリ５２１５のライセンス領域５２１５Ｂからライセンスを容易に取出し、メモリカード１１０へ移動できる。そして、ライセンスを移動した後は、メモリ５２１５のライセンス領域５２１５Ｂにおいて指定されたエントリ番号１内のライセンスは削除されるので、それに対応してライセンス管理ファイル１５２３のように「ライセンス無」が記録される。

【０２９９】また、ライセンス管理モジュール５１１によって受信された暗号化コンテンツデータのライセンスを格納する機密情報は、ライセンス管理ファイル１５２２，１５２４，・・・，１５２ｎによって管理される。ライセンス管理ファイル１５２２，・・・，１５２ｎは、ライセンス管理モジュール５１１によって受信した暗号化コンテンツデータを再生するためのライセンスを格納する機密情報の機密情報番号を含む。

【０３００】そうすると、たとえば、コンテンツファイル１５３２に記録されたファイル名の暗号化コンテンツデータをパーソナルコンピュータ８０へ移動させるとき、コンテンツファイル１５３１～１５３ｎを検索してコンテンツファイル１５３２を抽出し、コンテンツファイル１５３２に対応するライセンス管理ファイル１５２２から機密情報番号１を取得する。一方、ライセンス管理デバイス５２０からバインディング鍵Ｋｂを取得し、その取得したバインディング鍵Ｋｂによって暗号化機密ファイル１６０を復号して平文の機密ファイルを取得する。そうすると、ライセンス管理ファイルから取得した機密情報番号１に対応する機密ファイル中の機密情報１に格納されているライセンスを取得することができる。

【０３０１】このように、本発明の実施の形態１においては、ライセンス管理モジュール５１１によって受信した暗号化コンテンツデータのライセンスは、暗号化機密ファイル１６０に機密情報ｎとして格納されており、暗号化機密ファイル１６０は、ライセンス管理デバイス５２０によってハード的に保持されたバインディング鍵Ｋｂによってのみ復号可能である。つまり、バインディング鍵Ｋｂは、暗号化コンテンツデータのライセンスを管理する共通鍵であり、バインディング鍵Ｋｂがないとライセンスを取得することができない構造になっている。したがって、ライセンス管理モジュール５１１によって受信された暗号化コンテンツデータのライセンスは、暗号化機密ファイル１６０に書込まれてＨＤＤ５３０に記録されているため、実際はソフト的に管理されているが、ライセンス管理デバイス５２０に格納されたバインディング鍵Ｋｂがないとライセンスを暗号化機密ファイル１６０から取出すことができないわけでわるから、実質的には、ハードウエアによって管理されているのに近い。

【０３０２】一方、ライセンス管理デバイス５２０によって受信されたライセンスは、メモリ５２１５のライセンス領域５２１５Ｂに格納されている。したがって、本発明の実施の形態１によって、ライセンス管理モジュール５１１によって受信されたライセンスの管理レベル

を、ライセンス管理デバイス５２０によって受信されたライセンスの管理レベルに近づけることができる。

【０３０３】なお、バインディングライセンスは、エントリ番号「０」に格納されている物としている。

【０３０４】［移動１］図１に示すデータ配信システムにおいて、配信サーバ１０からパーソナルコンピュータ５０のライセンス管理デバイス５２０へ配信された暗号化コンテンツデータおよびライセンスを再生端末１００に装着されたメモリカード１１０へ送信する動作について説明する。なお、この動作を「移動１」という。移動は、セキュリティレベルがレベル２間でのみ行われる処理である図２６～図２９は、図１に示すデータ配信システムにおいて、ライセンス管理デバイス５２０が配信サーバ１０から受信した暗号化コンテンツデータおよびライセンスを再生端末１００に装着されたメモリカード１１０へ移動する移動動作を説明するための第１～第４のフローチャートである。

【０３０５】なお、図１８における処理以前に、パーソナルコンピュータ５０のユーザは、コンテンツリストファイルに従って、移動するコンテンツを決定し、ＨＤＤ５３０のコンテンツファイルおよびライセンス管理ファイルが特定でき、メモリカード１１０の再生リストファイルを取得していることを前提として説明する。

【０３０６】図２６を参照して、パーソナルコンピュータ５０のキーボード５６０から移動リクエストが入力されると（ステップＳ３００）、コントローラ５１０は、認証データの送信要求をＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して再生端末１００へ送信する（ステップＳ３０２）。そうすると、再生端末１００のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２およびバスＢＳ３を介して認証データの送信要求を受信し、バスＢＳ３およびメモリカードインタフェース１２００を介して認証データの送信要求をメモリカード１１０へ送信する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ４を介して認証データの送信要求を受信する（ステップＳ３０４）。

【０３０７】コントローラ１４２０は、認証データの送信要求を受信すると、認証データ保持部１４００から認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２をバスＢＳ４を介して読出し、その読出した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２をバスＢＳ４、インタフェース１４２４および端子１４２６を介して再生端末１００へ出力する。そして、再生端末１００のコントローラ１１０６は、メモリカードインタフェース１２００およびバスＢＳ３を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２を受取り、バスＢＳ３、ＵＳＢインタフェース１１１２、端子１１１４およびＵＳＢケーブル７０を介してパーソナルコンピュータ５０へ認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２を送信する（ステップＳ３０６）。

【０３０８】そうすると、パーソナルコンピュータ５０のコントローラ５１０は、端子５８０およびＵＳＢインタフェース５５０を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２を受信し（ステップＳ３０８）、その受信した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２をバスＢＳ２を介してライセンス管理デバイス５２０へ送信する。ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６、インタフェース５２２４、およびバスＢＳ５を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２を受信し、その受信した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２を復号処理部５２０８へ与える。認証処理部５２０８は、ＫＰａ保持部５２１４は、認証データ認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２を受取って、認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２に基づいて、ＫＰａ保持部５２１４からレベル２認証鍵ＫＰａ２を受取り、その受取ったレベル２認証鍵ＫＰａ２によって認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２の復号処理を実行する（ステップＳ３１０）。コントローラ５２２０は、復号処理部５２０８における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード１１０が正規のメモリカードからのクラス公開暗号鍵ＫＰｍ３とクラス証明書Ｃｍ３とを保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ３１２）。正当な認証データであると判断された場合、コントローラ５２２０は、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を承認し、受理する。そして、次の処理（ステップＳ３１４）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を受理しないで処理を終了する（ステップＳ４０４）。

【０３０９】認証の結果、正規のメモリカードであることが認識されると、コントローラ５２２０は、次に、メモリカード１１０のクラス証明書Ｃｍ３が禁止クラスリストＣＲＬにリストアップされているかどうかをメモリ５２１５のＣＲＬ領域５２１５Ａに照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで移動動作を終了する（ステップＳ４０４）。

【０３１０】一方、メモリカード１１０のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップＳ３１４）。

【０３１１】認証の結果、正当な認証データを持つメモリカードを備える再生端末からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、ライセンス管理デバイス５２０において、コントローラ５２２０は、移動を特定するための管理コードであるトランザクションＩＤをメモリ５２１５のライセンス

領域５２１５Ｂから取得する（ステップＳ３１６）。そして、セッションキー発生部５２１８は、移動のためのセッションキーＫｓ２２を生成する（ステップＳ３１８）。セッションキーＫｓ２２は、復号処理部５２０８によって得られたメモリカード１１０に対応するクラス公開暗号鍵ＫＰｍ３によって、暗号化処理部５２１０によって暗号化される（ステップＳ３２０）。コントローラ５２２０は、バスＢＳ５を介して暗号化データ｛Ｋｓ２２｝Ｋｍ３を取得し、メモリ５２１５から取得したトランザクションＩＤを暗号化データ｛Ｋｓ２２｝Ｋｍ３に追加したトランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３をバスＢＳ５、インタフェース５２２４および端子５２２６を介して出力する（ステップＳ３２２）。

【０３１２】図２７を参照して、パーソナルコンピュータ５０のコントローラ５１０は、バスＢＳ２を介してトランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３を受信し（ステップＳ３２４）、ＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介してトランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３を再生端末１００へ送信する（ステップＳ３２４）。そうすると、再生端末１００のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびＢＳ３を介してトランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３を受信し、その受信したトランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３をメモリカードインタフェース１２００を介してメモリカード１１０へ送信する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ４を介してトランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３を受信する（ステップＳ３２６）。復号処理部１４２２は、コントローラ１４２０からバスＢＳ４を介して｛Ｋｓ２２｝Ｋｍ３を受取り、Ｋｍ保持部１４２１からのクラス秘密復号鍵Ｋｍ３によって｛Ｋｓ２２｝Ｋｍ３を復号してセッションキーＫｓ２２を受理する（ステップＳ３２８）。そして、セッションキー発生部１４１８は、セッションキーＫｓ２を生成し（ステップＳ３３０）、コントローラ１４２０は、バスＢＳ４を介してメモリ１４１５のＣＲＬ領域１４１５Ａから禁止クラスリストの更新日時ＣＲＬｄａｔｅを取得し、その取得した更新日時ＣＲＬｄａｔｅを切換スイッチ１４４６へ与える（ステップＳ３３２）。

【０３１３】そうすると、暗号化処理部１４０６は、切換スイッチ１４４６の端子を順次切換えることによって取得したセッションキーＫｓ２、個別公開暗号鍵ＫＰｍｃ４および更新日時ＣＲＬｄａｔｅを、復号処理部１４０４によって復号されたセッションキーＫｓ２２によって暗号化し、暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２を生成する。コントローラ１４２０は、暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２をバスＢＳ４、インタフェース１４２４および端子１４２６を介して再生端末１００へ出力し、再生端末１００のコントローラ１１０６は、メモリカードインタフェース１２００を介して暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２を受取る。そして、コントローラ１１０６は、ＵＳＢインタフェース１１１２、端子１１１４、およびＵＳＢケーブル７０を介してパーソナルコンピュータ５０へ送信する（ステップＳ３３４）。

【０３１４】パーソナルコンピュータ５０のコントローラ５１０は、端子５８０およびＵＳＢインタフェース５５０を介して暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２を受信し（ステップＳ３３６）、バスＢＳ２を介して暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２をライセンス管理デバイス５２０へ入力する（ステップＳ３３８）。ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６、インタフェース５２２４およびバスＢＳ５を介して暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２を受信し、その受信した暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２を復号処理部５２１２に与える。復号処理部５２１２は、セッションキー発生部５２１８からのセッションキーＫｓ２２によって暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２を復号し、セッションキーＫｓ２、公開暗号鍵ＫＰｍｃ４および禁止クラスリストＣＲＬｄａｔｅを受理する（ステップＳ３４０）。

【０３１５】そうすると、パーソナルコンピュータ５０のコントローラ５１０は、ステップＳ３２４において、ライセンス管理ファイルに含まれるライセンスのエントリ番号をＨＤＤ５３０から読出す。そして、コントローラ５１０は、その読出したエントリ番号をバスＢＳ２を介してライセンス管理デバイス５２０に入力する（ステップＳ３４２）。ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６、インタフェース５２２４、およびバスＢＳ５を介してエントリ番号を受信し、メモリ５２１５のライセンス領域５２１５Ｂにおいて受信したエントリ番号によって指定された領域からライセンス（トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍ、再生期限ＡＣｐ）を読出す（ステップＳ３４４）。

【０３１６】アクセス制限情報ＡＣｍの受理に応じて、コントローラ５２２０は、アクセス制限情報ＡＣｍを確認する（ステップＳ３４６）。つまり、コントローラ５２２０は、取得したアクセス制限情報ＡＣｍのセキュリティレベル、再生回数、移動複製フラグについて順に判定を行う。最初に、アクセス制限情報ＡＣｍのセキュリティレベルとステップＳ３１０にて用いた認証鍵に基づいて、レベル１認証鍵ＫＰａ１を利用し、かつ、アクセス制限情報ＡＣｍのセキュリティレベルが２の場合に

は、ライセンスの管理要求レベルより低いセキュリティレベルへ出力となるので、ステップＳ４０４へ移行し、移動動作を中止する。それ以外の場合には次の判定を行う。アクセス制限情報ＡＣｍの再生回数に基づいて、再生端末１００に装着されたメモリカード１１０へ移動しようとするライセンスがアクセス制限情報ＡＣｍによって暗号化コンテンツデータの再生ができないライセンスになっていないか否かを確認する。再生回数がアクセス制限情報ＡＣｍによる制限回数に達している場合（＝０）、暗号化コンテンツデータをライセンスによって再生することができず、その暗号化コンテンツデータとライセンスとを再生端末１００に装着されたメモリカード１１０へ移動する意味がないからである。再生回数が「０」の場合に、ステップＳ４０４へ移行し、移動動作を中止する。それ以外（再生回数≠０）の場合には次の判定を行う。アクセス制限情報ＡＣｍの移動複製フラグに基づいて、移動複製禁止「＝０」のときステップＳ４０４並行し、移動動作を中止する。移動の為のときは、ステップＳ３４８並行し、そして、コントローラ５２２０は、メモリ５２１５のライセンス領域５２１５Ｂにおいて指定されたエントリ番号内のライセンスを削除して（ステップＳ３４８）、ステップＳ３５０並行する。移動複製可「＝２」のとき、ライセンスの複製であると判断され、ステップＳ３４８を行なわずにステップＳ３５０並行。

【０３１７】図２８を参照して、暗号化処理部５２１７は、復号処理部５２１２によって得られたライセンス管理デバイス５２０固有の個別公開暗号鍵ＫＰｍｃ４によってライセンスを暗号化して暗号化データ｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４を生成する（ステップＳ３５０）。そして、メモリカード１１０から送信された更新日時ＣＲＬｄａｔｅをライセンス管理デバイス５２０がＣＲＬ領域５２１５Ａに保持している禁止クラスリストの更新日時と比較し、いずれの禁止クラスリストが新しいかが判断され、メモカード１００の方が新しいと判断されたとき、ステップＳ３５２へ移行する。また、ライセンス管理デバイス５２０の方が新しいと判断されたときはステップＳ３６２へ移行する（ステップＳ３５２）。

【０３１８】データＣＲＬｄａｔｅが最新と判断されたとき、暗号化処理部５２０６は、暗号化処理部５２１７から出力された暗号化データ｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４をセッションキー発生部５２１８において発生されたセッションキーＫｓ２によって暗号化を行い、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２をバスＢＳ５に出力する。そして、コントローラ５２２０は、バスＢＳ５上の暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２をインタフェース５２２４および端子５２２６を介してパーソナルコンピュータ５０へ送信する（ステップＳ３５４）。

【０３１９】パーソナルコンピュータ５０のコントローラ５１０は、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受取り、ＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して再生端末１００へ送信する（ステップＳ３５６）。

【０３２０】再生端末１００のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介して暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受信し、その受信した暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２をバスＢＳ３およびメモリカードインタフェース１２００を介してメモリカード１１０へ送信する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、端子１４２４、およびバスＢＳ４を介して暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受信する（ステップＳ３５８）。

【０３２１】メモリカード１１０の復号処理部１４１２は、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２をバスＢＳ４を介して受取り、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２によって復号し、｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４を受理する（ステップＳ３６０）。その後、図２９に示すステップＳ３７６へ移行する。

【０３２２】一方、ステップＳ３５０において、ライセンス管理デバイス５２０の方が新しいと判断されると、ライセンス管理デバイス５２０のコントローラ５２２０は、バスＢＳ５を介してメモリ５２１５のＣＲＬ領域５２１５Ａから最新の禁止クラスリストＣＲＬを取得する（ステップＳ３６２）。

【０３２３】暗号化処理部５２０６は、暗号化処理部５２１７の出力と、コントローラ５２２０がバスＢＳ５を介してメモリ５２１５から取得した禁止クラスリストのデータＣＲＬとを、それぞれ、切換スイッチ５２４２および５２４６を介して受取り、セッションキー発生部５２１８において生成されたセッションキーＫｓ２によって暗号化する。暗号化処理部５２０６より出力された暗号化データ｛ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／インタフェース５２２４、および端子５２２６を介してパーソナルコンピュータ５０に出力される（ステップＳ３６４）。

【０３２４】パーソナルコンピュータ５０のコントロー

ラ５１０は、出力された暗号化データ｛ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受信し、ＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して暗号化データ｛ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を再生端末１００へ送信する（ステップＳ３６８）。再生端末１００のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介して暗号化データ｛ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受取り、バスＢＳ３およびメモリカードインタフェース１２００を介して暗号化データ｛ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２をメモリカード１１０へ送信する。そして、メモリカード１１００のコントローラ１４２０は、端子１４２６、インタフェース１４２４、およびバスＢＳ４を介して暗号化データ｛ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受信する（ステップＳ３７０）。

【０３２５】メモリカード１１０において、復号処理部１４１２は、セッションキー発生部１４１８から与えられたセッションキーＫｓ２を用いてバスＢＳ４上の受信データを復号し、ＣＲＬと｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４とを受理する（ステップ３７２）。コントローラ１４２０は、復号処理部１４１２によって受理されたデータＣＲＬをバスＢＳ４を介して受取り、その受取ったデータＣＲＬによってメモリ１４１５のＣＲＬ領域１４１５Ａを書換える（ステップＳ３７４）。

【０３２６】ステップＳ３５４，Ｓ３５６，Ｓ３５８，Ｓ３６０は、送信側のメモリカード１１０の禁止クラスリストＣＲＬが、受信側のライセンス管理デバイス５２０の禁止クラスリストＣＲＬより、新しい場合のライセンス鍵Ｋｃ等のメモリカード１１０への移動動作であり、ステップＳ３６２，Ｓ３６４，Ｓ３６８，Ｓ３７０，Ｓ３７２，Ｓ３７４は、送信側のライセンス管理デバイス５２０の禁止クラスリストＣＲＬが、受信側のメモリカード１１０の禁止クラスリストＣＲＬより、新しい場合のライセンス鍵Ｋｃ等のメモリカード１１０への移動動作である。このように、メモリカード１１０から送られてきた禁止クラスリストの更新日時ＣＲＬｄａｔｅによって、逐一、確認し、より最新の禁止クラスリストＣＲＬをメモリカード１１０の禁止クラスリストＣＲＬとしてＣＲＬ領域１５１４Ａに格納させることによって、クラス秘密鍵が漏洩などのセキュリティ機能の破られた機器へのライセンスの流出ををを防止できる。

【０３２７】図２９を参照して、ステップＳ３６０またはステップＳ３７４の後、コントローラ１４２０の指示によって、暗号化ライセンス｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４は、復号処理部１４０４において、個別秘密復号鍵Ｋｍｃ４によって復号され、ライセンス（ライセンス鍵Ｋｃ、トランザクションＩＤ、コンテンツＩＤ、アクセス制限情報ＡＣｍおよび再生期限ＡＣｐ）が受理される（ステップＳ３７６）。

【０３２８】このように、ライセンス管理デバイスおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、暗号化コンテンツデータおよびライセンスの移動動作におけるセキュリティを向上させることができる。

【０３２９】パーソナルコンピュータ５０のコントローラ５１０は、メモリカード１１０へ移動したライセンスを格納するためのエントリ番号を、ＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して再生端末１００へ送信する（ステップＳ３７８）。そうすると、再生端末１００のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介してエントリ番号を受取り、バスＢＳ３およびメモリカードインタフェース１２００を介してメモリカード１１０へ送信し、メモリカード１１０のコントローラ１４２０は、端子１４２６およびインタフェース１４２４を介してエントリ番号を受取り、その受取ったエントリ番号によって指定されるメモリ１４１５のライセンス領域１４１５Ｂに、ステップＳ３７６において取得したライセンス（ライセンス鍵Ｋｃ、トランザクションＩＤ、コンテンツＩＤ、アクセス制限情報ＡＣｍおよび再生期限ＡＣｐ）を格納する（ステップＳ３８０）。

【０３３０】パーソナルコンピュータ５０のコントローラ５１０は、メモリカード１１０のメモリ１４１５に格納されたライセンスのエントリ番号と、平文のトランザクションＩＤおよびコンテンツＩＤを含むメモリカード１１０へ移動しようとする暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆに対するライセンス管理ファイルを生成し、メモリカード１１０へ送信する（ステップＳ３８２）。

【０３３１】メモリカード１１０のコントローラ１４２０は、再生端末１００を介してライセンス管理ファイルを受信し、メモリ１４１５のデータ領域１４１５Ｃに受信したライセンス管理ファイルを記録する（ステップＳ３８４）。

【０３３２】そして、パーソナルコンピュータ５０のコントローラ５１０は、ステップＳ３４６の判断に従って、移動であればステップＳ３８８へ移行し、複製であ

65

ればステップＳ３８８を行なわないで、ステップＳ３９０並行する（ステップＳ３８６）。そして、移動の場合、ＨＤＤ５３０に記録されたライセンスのうち、メモリカード１１０へ移動したライセンスに対するライセンス管理ファイルのライセンスエントリ番号を、ライセンス無に更新する（ステップＳ３８６）。

【０３３３】その後、コントローラ５１０は、メモリカード１１０へ移動しようとするコンテンツファイル（暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆ）とをＨＤＤ５３０から取得し、｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆをメモリカード１１０へ送信する（ステップＳ３９０）。メモリカード１１０のコントローラ１４２０は、再生端末１００を介して｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆを受信し（ステップＳ３９２）、バスＢＳ４を介して受信した｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆをコンテンツファイルとしてメモリ１４１５のデータ領域１４１５Ｃに記録する（ステップＳ３９４）。

【０３３４】そうすると、パーソナルコンピュータ５０のコントローラ５１０は、メモリカード１１０へ移動した楽曲を追記した再生リストファイルを作成し（ステップＳ３９６）、再生リストファイルと、再生リストファイルの書換指示とをメモリカード１１０へ送信する（ステップＳ３９８）。メモリカード１１０のコントローラ１４２０は、再生端末１００を介して再生リストファイルと書換指示とを受信し（ステップＳ４００）、バスＢＳ４を介してメモリ１４１５のデータ領域１４１５Ｃに記録されている再生リストファイルを受信した再生リストファイルに書換え（ステップＳ４０２）、移動動作が終了する（ステップＳ４０４）。

【０３３５】なお、再生リストファイルとは、ＨＤＤに記録されていたコンテンツリストファイルと、同じ目的で作られた再生端末用の管理情報ファイルである。再生端末１００は、この再生リストファイルに含まれるコンテンツの登場順に、コンテンツファイルおよびライセンス管理ファイルを特定して再生を行なう。

【０３３６】このようにして、再生端末１００に装着されたメモリカード１１０が正規の機器であること、同時に、クラス証明書Ｃｍ３とともに暗号化して送信できた公開暗号鍵ＫＰｍ３が有効であることを確認した上で、クラス証明書Ｃｍ３が禁止クラスリスト、すなわち、公開暗号鍵ＫＰｍ３による暗号化が破られたクラス証明書リストに記載されていないメモリカードへの移動要求に対してのみコンテンツデータを移動することができ、不正なメモリカードへの移動および解読されたクラス鍵を用いた移動を禁止することができる。また、この移動動作を用いることによって、配信サーバ１０との通信機能を有さない再生端末１０２のユーザも、パーソナルコンピュータ５０を介して暗号化コンテンツデータおよびライセンスをメモリカードに受信することができ、ユーザの利便性は向上する。

66

【０３３７】また、説明から明らかなように移動処理として説明したが、コンテンツ供給者にとって、ライセンスの複製が許可されている場合には、複製処理として実行され、送信側のライセンス管理デバイス５１１にライセンスはそのまま保持される。この場合の複製は、配信時にコンテンツ供給者、すなわち、著作権所有者が複製を許可し、アクセス制限情報ＡＣｍの移動複製フラグを移動複製可に設定した場合にのみ許可される行為で含え居、著作権所有者の権利を阻害した行為ではない。アクセス制限情報はライセンスの一部であり、その機密性は保証されているにて、著作権は保護されている。

【０３３８】なお、上記においては、パーソナルコンピュータ５０のライセンス管理デバイス５２０からメモリカード１１０へのライセンスの移動について説明したが、メモリカード１１０からライセンス管理デバイス５２０へのライセンスの移動も、図２６～図２９に示すフローチャートに従って行なわれる。また、パーソナルコンピュータ５０が配信サーバ１０から受信した暗号化コンテンツデータおよびライセンスをメモリカード１１０へ移動できるのでは、ライセンス管理デバイス５２０が配信サーバ１０からハード的に受信した暗号化コンテンツデータおよびライセンスだけであり、ライセンス管理モジュール５１１が配信サーバ１０からソフト的に受信した暗号化コンテンツデータおよびライセンスを「移動」という概念によってメモリカードへ送信することはできない。ライセンス管理モジュール５１１は、ライセンス管理デバイス５２０よりも低いセキュリティレベルによってソフト的に配信サーバ１０との間で認証データおよび暗号鍵等のやり取りを行ない、暗号化コンテンツデータおよびライセンスを受信するので、その受信動作において暗号化が破られる可能性は、ライセンス管理デバイス５２０によって暗号化コンテンツデータおよびライセンスを受信する場合よりも高い。したがって、低いセキュリティレベルによって受信し、かつ、管理された暗号化コンテンツデータおよびライセンスを、ライセンス管理デバイス５２０と同じセキュリティレベルによって暗号化コンテンツデータおよびライセンスを受信して管理するメモリカード１１０へ「移動」という概念によって自由に移すことができるとすると、メモリカード１１０におけるセキュリティレベルが低下するので、これを防止するためにライセンス管理モジュール５１１によって受信した暗号化コンテンツデータおよびライセンスを「移動」という概念によってメモリカード１１０へ送信できなくしたものである。

【０３３９】しかしながら、ライセンス管理モジュール５１１によって受信されたセキュリティレベルの低い暗号化コンテンツデータおよびライセンスを、一切、メモリカード１１０へ移すことができないとすると、著作権を保護しながらコンテンツデータの自由なコピーを許容するデータ配信システムの趣旨に反し、ユーザの利便性

も向上しない。そこで、次に説明するチェックアウトおよびチェックインの概念によってライセンス管理モジュール５１１によって受信した暗号化コンテンツデータおよびライセンスをメモリカード１１０へ送信できるようにした。

【０３４０】［チェックアウト］図１に示すデータ配信システムにおいて、配信サーバ１０からパーソナルコンピュータ５０のライセンス管理モジュール５１１へ配信された暗号化コンテンツデータおよびライセンスを再生端末１００に装着されたメモリカード１１０に送信する動作について説明する。なお、この動作を「チェックアウト」という。

【０３４１】図３０～図３４は、図１に示すデータ配信システムにおいて、ライセンス管理モジュール５１１が配信サーバ１０から受信した暗号化コンテンツデータおよびライセンスを、返却を条件として再生端末１００に装着されたメモリカード１１０へ貸出すチェックアウト動作を説明するための第１～第５のフローチャートである。なお、図３０における処理以前に、パーソナルコンピュータ５０のユーザは、コンテンツリストファイルに従って、チェックアウトするコンテンツを決定し、ＨＤＤ５３０のコンテンツファイルおよびライセンス管理ファイルが特定でき、メモリカード１１０の再生リストファイルを取得していることを前提として説明する。

【０３４２】図３０を参照して、パーソナルコンピュータ５０のキーボード５６０からチェックアウトリクエストが入力されると（ステップＳ５００）、ライセンス管理モジュール５１１は、バインディング鍵取得処理を行う。図３０のステップＳ５０１から図３１のステップＳ１５の一連の処理がバインディング鍵取得処理であり、配信２のフローチャートにおける図２０のステップＳ２７０から図２１のステップＳ２８４の一連の処理と同じである。ゆえに、説明を省略する。

【０３４３】バインディング鍵Ｋｂを取得したライセンス管理モジュール５１１は、バスＢＳ２を介してＨＤＤ５３０から暗号化機密ファイル１６０を取得し、その取得した暗号化機密ファイル１６０をバインディング鍵Ｋｂによって復号して平文の機密ファイルを取得する（ステップＳ５１６）。その後、ライセンス管理モジュール５１１は、ライセンス管理ファイルに記録された機密情報番号ｎに対応する機密ファイル内の機密情報ｎ（トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍ、再生期限ＡＣｐ、およびチェックアウト情報）を取得する（ステップＳ５１７）。

【０３４４】そうすると、ライセンス管理モジュール５１１は、取得したアクセス制限情報ＡＣｍに基づいてライセンスがチェックアウト可能か否かを確認する（ステップＳ５１８）、つまり、ライセンス管理モジュール５１１は、再生端末１００に装着されたメモリカード１１０へチェックアウトしようとするライセンスがアクセス制限情報ＡＣｍの再生回数によって暗号化コンテンツデータの再生回数の制限がないか、再生ができないライセンスになっていないか否かを確認する。再生回数に制限がある場合、暗号化コンテンツデータおよびライセンスをチェックアウトしない。

【０３４５】ステップＳ５１８において、再生に制限がある場合、ステップＳ５６４へ移行し、チェックアウト動作は終了する。ステップＳ５１８において、暗号化コンテンツデータの再生回数がアクセス制限情報ＡＣｍによる制限回数に達していない場合、ステップＳ５１９へ移行する。そして、ライセンス管理モジュール５１１は、取得したチェックアウト情報に含まれるチェックアウト可能数が「０」よりも大きいか否かを確認する（ステップＳ５１９）。ステップＳ５１９において、チェックアウト可能数が「０」であれば、チェックアウトできるライセンスが無いので、ステップＳ５６４へ移行し、チェックアウト動作は終了する。ステップＳ５１９において、チェックアウト可能数が「０」よりも大きいとき、ライセンス管理モジュール５１１は、ＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して認証データの送信要求を送信する（ステップＳ５２０）。再生端末１００のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介して認証データの送信要求を受信し、その受信した認証データの送信要求をバスＢＳ３およびメモリカードインタフェース１２００を介してメモリカード１１０へ送信する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ４を介して認証データの送信要求を受信する（ステップＳ５２１）。

【０３４６】コントローラ１４２０は、認証データの送信要求を受信すると、認証データ保持部１４００から認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２をバスＢＳ４を介して読出し、その読出した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２をバスＢＳ４、インタフェース１４２４および端子１４２６を介して再生端末１００へ出力する。そして、再生端末１００のコントローラ１１０６は、メモリカードインタフェース１２００およびバスＢＳ３を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２を受取り、バスＢＳ３、ＵＳＢインタフェース１１１２、端子１１１４およびＵＳＢケーブル７０を介してパーソナルコンピュータ５０へ認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２を送信する（ステップＳ５２２）。

【０３４７】そうすると、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、端子５８０およびＵＳＢインタフェース５５０を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２を受信し（ステップＳ５２３）、その受信した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２をレベル２認証鍵ＫＰａ２によって復号する

（ステップＳ５２４）。

【０３４８】図３２を参照して、ライセンス管理モジュール５１１は、復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード１１０が正規のメモリカードからのクラス公開暗号鍵ＫＰｍ３とクラス証明書Ｃｍ３とを保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ５２５）。正当な認証データであると判断された場合、ライセンス管理モジュール５１１は、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を承認し、受理する。そして、次の処理（ステップＳ５２６）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を受理しないで処理を終了する（ステップＳ５６４）。

【０３４９】認証の結果、正規のメモリカードであることが認識されると、ライセンス管理モジュール５１１は、次に、メモリカード１１０のクラス証明書Ｃｍ３が禁止クラスリストＣＲＬにリストアップされているかどうかをＨＤＤ５３０に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここでチェックアウト動作を終了する（ステップＳ５６４）。一方、メモリカード１１０のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップＳ５２６）。

【０３５０】認証の結果、正当な認証データを持つメモリカードを備える再生端末からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、ライセンス管理モジュール５１１は、チェックアウトを特定するための管理コードであるチェックアウト用トランザクションＩＤを、メモリカード１１０の格納されている全てのトランザクションＩＤと異なる値をとり、かつ、ローカル使用のトランザクションＩＤとして生成する。生成する（ステップＳ５２７）。そして、ライセンス管理モジュール５１１は、チェックアウトのためのセッションキーＫｓ２ｂを生成し（ステップＳ５２８）、メモリカード１１０から送信されたクラス公開暗号鍵ＫＰｍ３によって、生成したセッションキーＫｓ２ｂを暗号化する（ステップＳ５２９）。そして、ライセンス管理モジュール５１１は、暗号化データ｛Ｋｓ２ｂ｝Ｋｍ３にチェックアウト用トランザクションＩＤを追加したチェックアウト用トランザクションＩＤ／／｛Ｋｓ２ｂ｝Ｋｍ３をＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して再生端末１００へ送信する（ステップＳ５３０）。そうすると、再生端末１００のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介してチェックアウト用トランザクションＩＤ／／｛Ｋｓ２ｂ｝Ｋｍ３を受信し、その受信したチェックアウト用トランザクションＩＤ／／｛Ｋｓ２ｂ｝Ｋｍ３をメモリカードインタフェース１２００を介してメモリカード１１０へ送信する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ４を介してチェックアウト用トランザクションＩＤ／／｛Ｋｓ２ｂ｝Ｋｍ３を受信する（ステップＳ５３１）。復号処理部１４２２は、コントローラ１４２０からバスＢＳ４を介して｛Ｋｓ２ｂ｝Ｋｍ３を受取り、Ｋｍ保持部１４２１からの秘密復号鍵Ｋｍ３によって｛Ｋｓ２ｂ｝Ｋｍ３を復号してセッションキーＫｓ２ｂを受理する（ステップＳ５３２）。そして、セッションキー発生部１４１８は、セッションキーＫｓ２ｃを生成し（ステップＳ５３３）、コントローラ１４２０は、バスＢＳ４を介してメモリ１４１５のＣＲＬ領域１４１５Ａから禁止クラスリストの更新日時ＣＲＬｄａｔｅを取得し、その取得した更新日時ＣＲＬｄａｔｅを切換スイッチ１４４６へ与える（ステップＳ５３４）。

【０３５１】そうすると、暗号化処理部１４０６は、切換スイッチ１４４６の端子を順次切換えることによって取得したセッションキーＫｓ２ｃ、個別公開暗号鍵ＫＰｍｃ４および更新日時ＣＲＬｄａｔｅを、復号処理部１４０４によって復号されたセッションキーＫｓ２ｂによって暗号化し、暗号化データ｛Ｋｓ２ｃ／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２ｂを生成する。コントローラ１４２０は、暗号化データ｛Ｋｓ２ｃ／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２ｂをバスＢＳ４、インタフェース１４２４および端子１４２６を介して再生端末１００へ出力し、再生端末１００のコントローラ１１０６は、メモリカードインタフェース１２００を介して暗号化データ｛Ｋｓ２ｃ／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２ｂを受取る。そして、コントローラ１１０６は、ＵＳＢインタフェース１１１２、端子１１１４、およびＵＳＢケーブル７０を介してパーソナルコンピュータ５０へ送信する（ステップＳ５３５）。

【０３５２】パーソナルコンピュータ５０のライセンス管理モジュール５１１は、端子５８０およびＵＳＢインタフェース５５０を介して暗号化データ｛Ｋｓ２ｃ／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２ｂを受信し（ステップＳ５３６）、その受信した暗号化データ｛Ｋｓ２ｃ／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２ｂをセッションキーＫｓ２ｂによって復号し、セッションキーＫｓ２ｃ、個別公開暗号鍵ＫＰｍｃ４および更新日時ＣＲＬｄａｔｅを受理する（ステップＳ５３７）。そして、ライセンス管理モジュール５１１は、再生端末１００に装着されたメモリカードから他のメモリカード等へライセンスが移動／複製されるのを禁止したチェックアウト用アクセス制限情報ＡＣｍを生成する。すなわち、再生回数を無制限（＝２５５）、移動複製フラグを移動複製不可（＝３）、セキュリティレベルを１に設定したアク

セス制限情報ＡＣｍを生成する（ステップＳ５３８）。

【０３５３】図３３を参照して、ライセンス管理モジュール５１１は、ステップＳ５３７において受信したメモリカード１１０に固有の公開暗号鍵ＫＰｍｃ４によってライセンスを暗号化して暗号化データ｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４を生成する（ステップＳ５３９）。そして、メモリカード１１０から送信された更新日時ＣＲＬｄａｔｅが、ライセンス管理モジュール５１１が管理するＨＤＤ５３０に保持される禁止クラスリストの更新日時と比較し、いずれの禁止クラスリストが新しいかが判断され、メモリカード１１０の方が新しいと判断されたとき、ステップＳ５４１へ移行する。また、逆に、ライセンス管理モジュール５１１の方が新しいと判断されたときはステップＳ５４４へ移行する（ステップＳ５４０）。

【０３５４】メモリカード１１０の方が新しいと判断されたとき、ライセンス管理モジュール５１１は、暗号化データ｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４をセッションキーＫｓ２ｃによって暗号化を行い、暗号化データ｛｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｃをＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して再生端末１００へ送信する（ステップＳ５４１）。

【０３５５】再生端末１００のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介して暗号化データ｛｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｃを受信し、その受信した暗号化データ｛｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｃをバスＢＳ３およびメモリカードインタフェース１２００を介してメモリカード１１０へ送信する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、端子１４２４、およびバスＢＳ４を介して暗号化データ｛｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｃを受信する（ステップＳ５４２）。

【０３５６】メモリカード１１０の復号処理部１４１２は、暗号化データ｛｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｃをバスＢＳ４を介して受取り、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２ｃによって復号し、｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４を受理する（ステップＳ５４３）。その後、図３４に示すステップＳ５４９へ移行する。

【０３５７】一方、ステップＳ５４０において、ライセンス管理モジュール５１１の禁止クラスリストのほうが新しいと判断されると、ライセンス管理モジュール５１１は、ＨＤＤ５３０からライセンス管理モジュール５１１の管理する禁止クラスリストＣＲＬを取得する（ステップＳ５４４）。

【０３５８】そして、ライセンス管理モジュール５１１は、｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４と、ＨＤＤ５３０から取得した禁止クラスリストのデータＣＲＬとをセッションキーＫｓ２ｃによって暗号化し、その暗号化データ｛ＣＲＬ／／｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｃをＵＳＢインタフェース５５０、端子５８０およびＵＳＢケーブル７０を介して再生端末１００へ送信する（ステップＳ５４５）。再生端末１００のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介して暗号化データ｛ＣＲＬ／／｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｃを受信し、その受信した暗号化データ｛ＣＲＬ／／｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｃをバスＢＳ３およびメモリカードインタフェース１２００を介してメモリカード１１０へ出力する。そうすると、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４、およびバスＢＳ４を介して暗号化データ｛ＣＲＬ／／｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｃを受信する（ステップＳ５４６）。

【０３５９】メモリカード１１０において、復号処理部１４１２は、セッションキー発生部１４１８から与えられたセッションキーＫｓ２ｃを用いてバスＢＳ４上の受信データを復号し、ＣＲＬと｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４とを受理する（ステップＳ５４７）。コントローラ１４２０は、復号処理部１４１２によって受理されたデータＣＲＬをバスＢＳ４を介して受取り、その受取ったデータＣＲＬによってメモリ１４１５のＣＲＬ領域１４１５Ａを書換える（ステップＳ５４８）。

【０３６０】ステップＳ５４１、Ｓ５４２、Ｓ５４３は、送信側のライセンス管理モジュール５１１の禁止クラスリストＣＲＬより、受信側のメモリカード１１０の

禁止クラスリストＣＲＬが新しい場合のライセンス鍵Ｋｃ等のメモリカード１１０へのチェックアウト動作であり、ステップＳ５４４，Ｓ５４５，Ｓ５４６，Ｓ５４７，Ｓ５４８は、受信側のメモリカード１１０の禁止クラスリストＣＲＬより、送信側のライセンス管理モジュール５１１の禁止クラスリストＣＲＬが新しい場合のライセンス鍵Ｋｃ等のメモリカード１１０へのチェックアウト動作である。このように、メモリカード１１０へライセンスを送信するときに、メモリカード１００がＣＲＬ領域１４１５Ｂで保持する禁止クラスリストＣＲＬより、ＨＤＤ５３０に新しい禁止クラスリストＣＲＬが記録されている場合には禁止クラスリストＣＲＬをＨＤＤ５３０から取得し、禁止クラスリストＣＲＬをメモリカード１１０に配信することによって、メモリカード１００がＣＲＬ領域１４１５Ｂで保持する禁止クラスリストを更新していくことができる、クラス鍵が破られたメモリカード１１０へのらい線への送信を禁止することができ、配信されたライセンスの流出を防止できる。

【０３６１】図３４を参照して、ステップＳ５４３またはステップＳ５４８の後、コントローラ１４２０の指示によって、暗号化ライセンス（チェックアウト用トランザクション１Ｄ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ）Ｋｍｃ４は、復号処理部１４０４において、秘密復号鍵Ｋｍｃ４によって復号され、ライセンス（ライセンス鍵Ｋｃ、チェックアウト用トランザクションＩＤ、コンテンツＩＤ、チェックアウト用ＡＣｍおよび再生期限ＡＣｐ）が受理される（ステップＳ５４９）。

【０３６２】そして、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、メモリカード１１０へチェックアウトしたライセンスを格納するためのエントリ番号を、ＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して再生端末１０２へ送信します（ステップＳ５５０）。そうすると、再生端末１０２のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介してエントリ番号を受取り、その受取ったエントリ番号によって指定されるメモリ１４１５のライセンス領域１４１５Ｂに、ステップＳ５６６において受理したライセンス（ライセンス鍵Ｋｃ、チェックアウト用トランザクションＩＤ、コンテンツＩＤ、チェックアウト用ＡＣｍおよび再生制御情報ＡＣｐ）を格納する（ステップＳ５５１）。

【０３６３】パーソナルコンピュータ５０のライセンス管理モジュール５１１は、メモリカード１１０のメモリ１４１５に格納されたライセンスのエントリ番号と、平文のチェックアウト用トランザクションＩＤおよびコンテンツＩＤを含むメモリカード１１０へ移動しようとする暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆに対するライセンス管理ファイルを生成し、メモリカード１１０へ送信する（ステップＳ５５２）。

【０３６４】メモリカード１１０のコントローラ１４２０は、再生端末１０２を介してライセンス管理ファイルを受信し、メモリ１４１５のデータ領域１４１５Ｃに受信したライセンス管理ファイルを記録する（ステップＳ５５３）。

【０３６５】パーソナルコンピュータ５０のライセンス管理モジュール５１１は、チェックアウト可能数を１減算し、チェックアウト用トランザクションＩＤとチェックアウト先のメモリカードに固有の公開暗号鍵ＫＰｍｃ４とを追加してチェックアウト情報を更新する（ステップＳ５５４）。そして、ライセンス管理モジュール５１１は、トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍ、再生期限ＡＣｐ、および更新したアドレス情報（チェックアウト可能数と、チェックアウト用トランザクションＩＤと、チェックアウト先のメモリカード１１０に個別の戸別公開暗号鍵ＫＰｍｃ４を追加したもの）を新たな機密情報ｎとして平文の機密ファイルを更新する（ステップＳ５５５）。チェックアウト先の個別公開鍵ＫＰｍｃ４は、個別公開鍵はメモリカードの耐タンパモジュール無いに格納され、かつ、認証による暗号を用いたセキュリティの高い通信手段によって入手するメモリカードごとに固有値を持つため、メモリカード特定する識別情報として適している。

【０３６６】その後、ライセンス管理モジュール５１１は、平文の機密ファイルをバインディング鍵Ｋｂによって暗号化してＨＤＤ５３０に記録されている暗号化機密ファイル１６０を更新する（ステップＳ５５６）。

【０３６７】ライセンス管理モジュール５１１は、メモリカード１１０へチェックアウトしようとする暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆとをＨＤＤ５３０から取得し、｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆをメモリカード１１０へ送信する（ステップＳ５５７）。メモリカード１１０のコントローラ１４２０は、再生端末１００を介して｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆを受信し（ステップＳ５５８）、バスＢＳ４を介して受信した｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆをメモリ１４１５のデータ領域１４１５Ｃに記録する（ステップＳ５５９）。

【０３６８】そうすると、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、メモリカード１１０へチェックアウトした楽曲を追記した再生リストファイルを作成し（ステップＳ５６０）、再生リストファイルと、再生リストファイルとの書換指示とをメモリカード１１０へ送信する（ステップＳ５６１）。メモリカード１１０のコントローラ１４２０は、再生端末１００を介して再生リストと書換指示とを受信し（ステップＳ５６２）、バスＢＳ４を介してメモリ１４１５のデータ領域１４１５Ｃに記録されている再生リストファイルを

受信した再生リストファイルに書換え（ステップＳ５６３）、チェックアウト動作が終了する（ステップＳ５６４）。

【０３６９】このようにして、再生端末１００に装着されたメモリカード１１０が正規の機器であること、同時に、クラス証明書Ｃｍ３とともに暗号化して送信されたクラス公開暗号鍵ＫＰｍ３が有効であることを確認した上で、クラス証明書Ｃｍ３が禁止クラスリスト、すなわち、クラス公開暗号鍵ＫＰｍ３による暗号化が破られたクラス証明書リストに記載されていないメモリカードへのチェックアウト要求に対してのみコンテンツデータをチェックアウトすることができ、不正なメモリカードへのチェックアウトおよび解読されたクラス鍵を用いたチェックアウトを禁止することができる。また、ライセンス管理モジュールおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、暗号化コンテンツデータおよびライセンスのチェックアウト動作におけるセキュリティを向上させることができる。さらに、このチェックアウト動作を用いることによって、配信サーバ１０との通信機能を有さない再生端末１００のユーザも、パーソナルコンピュータ５０がソフトウエアによって受信した暗号化コンテンツデータおよびライセンスをメモリカードに受信することができ、ユーザの利便性は向上する。

【０３７０】［チェックイン］図１に示すデータ配信システムにおいて、パーソナルコンピュータ５０のライセンス管理モジュール５１１からメモリカード１１０へチェックアウトされた暗号化コンテンツデータおよびライセンスをライセンス管理モジュール５１１へ戻す動作について説明する。なお、この動作を「チェックイン」という。

【０３７１】図３５～図３８は、図３０～図３４を参照して説明したチェックアウト動作によってメモリカード１１０へ貸出された暗号化コンテンツデータおよびライセンスを返却して貰うチェックイン動作を説明するための第１～第４のフローチャートである。なお、図３５における処理以前に、パーソナルコンピュータ５０のユーザは、ＨＤＤ５２０に記録されているコンテンツリストファイルとメモリカード１１０のデータ領域１４１５Ｂに記録されている再生リストファイルを取得し、両ファイルに従って、チェックインするコンテンツを決定し、ＨＤＤ５３０およびメモカード１１０のコンテンツファイルおよびライセンス管理ファイルが特定でき、かつ、メモリカード１１０のライセンス管理ファイルを取得してていることを前提として説明する。

【０３７２】図３５を参照して、パーソナルコンピュータ５０のキーボード５６０からチェックインリクエストが入力されると（ステップＳ６００）、ライセンス管理モジュール５１１は、バインディング鍵取得処理を行う。図３５のステップＳ６０１から図３６のステップ６１５の一連の処理がバインディング鍵取得処理であり、配信２のフローチャートにおける図２０のステップＳ２７０から図２１のステップＳ２８４の一連の処理と同じである。ゆえに、説明を省略する。

【０３７３】バインディング鍵Ｋｂを取得したライセンス管理モジュール５１１は、バスＢＳ２を介してＨＤＤ５３０から暗号化機密ファイル１６０を取得し、その取得した暗号化機密ファイル１６０をバインディング鍵Ｋｂによって復号して平文の機密ファイルを取得する（ステップＳ６１６）。その後、ライセンス管理モジュール５１１は、ライセンス管理ファイルに記録された機密情報番号ｎに対応する機密ファイル内の機密情報ｎ（ライセンス（トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍ、再生期限ＡＣｐ）、およびチェックアウト情報（チェックアウト可能数、チェックアウト用トランザクションＩＤ、チェックアウト先のメモリカードの個別公開暗号鍵ＫＰｍｃｘ））を取得する（ステップＳ６１７）。そして、ライセンス管理モジュール５１１は、認証データの送信要求をＵＳＢインターフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して再生端末１００へ送信する（ステップＳ６１８）。

【０３７４】そうすると、再生端末１００のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２およびバスＢＳ３を介して認証データの送信要求を受信し、バスＢＳ３およびメモリカードインタフェース１２００を介して認証データの送信要求をメモリカード１１０へ送信する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ４を介して認証データの送信要求を受信する（ステップＳ６１９）。

【０３７５】コントローラ１４２０は、認証データの送信要求を受信すると、認証データ保持部１４００から認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２をバスＢＳ４を介して読出し、その読出した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２をバスＢＳ４、インタフェース１４２４および端子１４２６を介して再生端末１００へ出力する。そして、再生端末１００のコントローラ１１０６は、メモリカードインタフェース１２００およびバスＢＳ３を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２を受取り、バスＢＳ３、ＵＳＢインタフェース１１１２、端子１１１４およびＵＳＢケーブル７０を介してパーソナルコンピュータ５０へ認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２を送信する（ステップＳ６２０）。

【０３７６】パーソナルコンピュータ５０のライセンス管理モジュール５１１は、端子５８０およびＵＳＢインタフェース５５０を介して認証データ｛ＫＰｍ３／／Ｃ

ｍ３｝ＫＰａ２を受信し（ステップＳ６２１）、その受信した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２をレベル２認証鍵ＫＰａによって復号する（ステップＳ６２２）。そして、ライセンス管理モジュール５１１は、復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード１１０が正規のメモリカードからのクラス公開暗号鍵ＫＰｍ３とクラス証明書Ｃｍ３とを保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行う（ステップＳ６２３）。正当な認証データであると判断された場合、ライセンス管理モジュール５１１は、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を承認し、受理する。そして、次の処理（ステップＳ６２４）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を受理しないで処理を終了する（ステップＳ６５３）。認証の結果、正規のメモリカードであることが認識されると、ライセンス管理モジュール５１１は、ダミートランザクションＩＤを生成する（ステップＳ６２４）。ダミー用トランザクションＩＤは、必ず、メモリカード１１０の格納されている全てのトランザクションＩＤと異なる値をとり、かつ、ローカル使用のトランザクションＩＤとして生成する。

【０３７７】図３７を参照して、ライセンス管理モジュール５１１は、チェックイン用のセッションキーＫｓ２ｂを生成する（ステップＳ６２５）。そして、ライセンス管理モジュール５１１は、生成したセッションキーＫｓ２ｂをメモリカード１１０から受信したクラス公開暗号鍵ＫＰｍ３によって暗号化し、暗号化データ｛Ｋｓ２ｂ｝Ｋｍ３を生成し（ステップＳ６２６）、暗号化データ｛Ｋｓ２ｂ｝Ｋｍ３とダミートランザクションＩＤを追加したダミートランザクションＩＤ／／｛Ｋｓ２ｂ｝Ｋｍ３をＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して再生端末１００へ送信する（ステップＳ６２７）。再生端末１００のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびＢＳ３を介してダミートランザクションＩＤ／／｛Ｋｓ２ｂ｝Ｋｍ３を受信し、その受信したダミートランザクションＩＤ／／｛Ｋｓ２ｂ｝Ｋｍ３をメモリカードインタフェース１２００を介してメモリカード１１０へ送信する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ４を介してダミートランザクションＩＤ／／｛Ｋｓ２ｂ｝Ｋｍ３を受信する（ステップＳ６２８）。復号処理部１４２２は、コントローラ１４２０からバスＢＳ４を介して｛Ｋｓ２ｂ｝Ｋｍ３を受取り、Ｋｍ保持部１４２１からのクラス秘密復号鍵Ｋｍ３によって｛Ｋｓ２ｂ｝Ｋｍ３を復号してセッションキーＫｓ２ｂを受理する（ステップＳ６２９）。そして、セッションキー発生部１４１８は、セッションキーＫｓ２ｃを生成し（ステップＳ６３０）、コントローラ１４２０は、バスＢＳ４を介してメモリ１４１５のＣＲＬ領域１４１５Ａから禁止クラスリストの更新日時ＣＲＬｄａｔｅを取得し、その取得した更新日時ＣＲＬｄａｔｅを切換スイッチ１４４６へ与える（ステップＳ６３１）。

【０３７８】そうすると、暗号化処理部１４０６は、切換スイッチ１４４６の端子を順次切換えることによって取得したセッションキーＫｓ２ｃ、個別公開暗号鍵ＫＰｍｃ４および更新日時ＣＲＬｄａｔｅを、復号処理部１４２２によって復号され、切換スイッチ１４４２の端子Ｐａを介して取得したセッションキーＫｓ２ｂによって暗号化し、暗号化データ｛Ｋｓ２ｃ／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２ｂを生成する。コントローラ１４２０は、暗号化データ｛Ｋｓ２ｃ／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２ｂをバスＢＳ４、インタフェース１４２４および端子１４２６を介して再生端末１００へ出力し、再生端末１００のコントローラ１１０６は、メモリカードインタフェース１２００を介して暗号化データ｛Ｋｓ２ｃ／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２ｂを受取る。そして、コントローラ１１０６は、暗号化データ｛Ｋｓ２ｃ／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２ｂをＵＳＢインタフェース１１１２、端子１１１４、およびＵＳＢケーブル７０を介してパーソナルコンピュータ５０へ送信する（ステップＳ６３２）。

【０３７９】パーソナルコンピュータ５０のライセンス管理モジュール５１１は、端子５８０およびＵＳＢインタフェース５５０を介して暗号化データ｛Ｋｓ２ｃ／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２ｂを受信し（ステップＳ６３３）、その受信した暗号化データ｛Ｋｓ２ｃ／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２ｂをセッションキーＫｓ２ｂによって復号し、セッションキーＫｓ２ｃ、個別公開暗号鍵ＫＰｍｃ４および更新日時ＣＲＬｄａｔｅを受理する（ステップＳ６３４）。

【０３８０】そうすると、ライセンス管理モジュール５１１は、受理した個別公開暗号鍵ＫＰｍｃ４がステップＳ６１７で取得した機密情報ｎのチェックアウト情報に含まれる否かを、すなわち、チェックアウトしようとするライセンスのチェックアウト用トランザクションＩＤに対応して格納されている個別公開暗号鍵ＫＰｍｃｘと一致するか否かを確認する（ステップＳ６３５）。

【０３８１】受理された個別公開暗号鍵ＫＰｍｃ４は、暗号化コンテンツデータおよびライセンスのチェックアウトの際に、更新されたチェックアウト情報に含まれるものである（図３４のステップＳ５５１を参照）。したがって、暗号化コンテンツデータ等のチェックアウト先に対応する個別公開暗号鍵ＫＰｍｃ４をチェックアウト情報に含ませることによってチェックインの際にチェックアウトしたチェックアウト先を容易に特定することが

できる。

【０３８２】ステップＳ６３５において、個別公開暗号鍵ＫＰｍｃ４がチェックアウト情報に含まれていないときチェックイン動作は終了する（ステップＳ６５３）。ステップＳ６３５において、個別公開暗号鍵ＫＰｍｃ４がチェックアウト情報に含まれていると、ライセンス管理モジュール５１１は、ダミーライセンス、つまり、ダミートランザクションＩＤ、対応するコンテンツ存在しないダミーコンテンツＩＤ、再生に関与し得ないダミーライセンス鍵Ｋｃ（ダミーＫｃと表す。）、移動複製フラグが「移動複製禁止」かつ再生回数が「０」を示すダミーアクセス制限情報ＡＣｍ（ダミーＡＣｍと表す。）、およびダミー再生期限ＡＣｐ（ダミーＡＣｐと表す。）を個別公開暗号鍵ＫＰｍｃ４によって暗号化し、暗号化データ｛ダミートランザクションＩＤ／／ダミーコンテンツＩＤ／／Ｋｃ／／ダミーＡＣｍ／／ダミーＡＣｐ｝Ｋｍｃ４を生成する（ステップＳ６３６）。

【０３８３】ライセンス管理モジュール５１１は、暗号化データ｛ダミートランザクションＩＤ／／ダミーコンテンツＩＤ／／ダミーＫｃ／／ダミーＡＣｍ／／ダミーＡＣｐ｝Ｋｍｃ４をセッションキーＫｓ２ｃによって暗号化を行い、暗号化データ｛｛ダミートランザクションＩＤ／／ダミーコンテンツＩＤ／／ダミーＫｃ／／ダミーＡＣｍ／／ダミーＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｃを生成し、その生成した暗号化データ｛｛ダミートランザクションＩＤ／／ダミーコンテンツＩＤ／／Ｋｃ／／ダミーＡＣｍ／／ダミーＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｃをＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して再生端末１００へ送信する（ステップＳ６３７）。

【０３８４】再生端末１００のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介して暗号化データ｛｛ダミートランザクションＩＤ／／ダミーコンテンツＩＤ／／ダミーＫｃ／／ダミーＡＣｍ／／ダミーＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｃを受信する。コントローラ１１０６は、受信した暗号化データ｛｛ダミートランザクションＩＤ／／ダミーコンテンツＩＤ／／ダミーＫｃ／／ダミーＡＣｍ／／ダミーＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｃをバスＢＳ３およびメモリカードインタフェース１２００を介してメモリカード１１０へ送信する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、端子１４２４、およびバスＢＳ４を介して｛｛ダミートランザクションＩＤ／／ダミーコンテンツＩＤ／／ダミーＫｃ／／ダミーＡＣｍ／／ダミーＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｃを受信する（ステップＳ６３８）。

【０３８５】図３８を参照して、メモリカード１１０の復号処理部１４１２は、｛｛ダミートランザクションＩＤ／／ダミーコンテンツＩＤ／／ダミーＫｃ／／ダミーＡＣｍ／／ダミーＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｃをバスＢＳ４を介して受取り、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２ｃによって復号し、｛ダミートランザクションＩＤ／／ダミーコンテンツＩＤ／／ダミーＫｃ／／ダミーＡＣｍ／／ダミーＡＣｐ｝Ｋｍｃ４を受理する（ステップＳ６３９）。そして、復号処理部１４０４は、暗号化データ｛ダミートランザクションＩＤ／／ダミーコンテンツＩＤ／／ダミーＫｃ／／ダミーＡＣｍ／／ダミーＡＣｐ｝Ｋｍｃ４を復号処理部１４１２から受取り、その受取った暗号化データ｛ダミートランザクションＩＤ／／ダミーコンテンツＩＤ／／ダミーＫｃ／／ダミーＡＣｍ／／ダミーＡＣｐ｝Ｋｍｃ４をＫｍｃ保持部１４０２からの個別秘密復号鍵Ｋｍｃ４によって復号し、ダミートランザクションＩＤ、ダミーコンテンツＩＤ、ダミーＫｃ、ダミーＡＣｍ、およびダミーＡＣｐを受理する（ステップＳ６４０）。

【０３８６】パーソナルコンピュータ５０のライセンス管理モジュール５１１は、メモリカードＩＤのライセンス管理ファイルに記載されているチェックアウトするライセンスが格納されているエントリ番号を取得して、ダミーライセンスを格納するためのエントリ番号として、ＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して再生端末１０２へ送信する（ステップＳ６４１）。そうすると、再生端末１０２のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介してエントリ番号を受取り、バスＢＳ４を介してその受取ったエントリ番号によって指定されるメモリ１４１５のライセンス領域１４１５Ｂに、ダミーライセンス（ダミートランザクションＩＤ、ダミーコンテンツＩＤ、ダミーライセンス鍵Ｋｃ、ダミーアクセス制限情報ＡＣｍ、およびダミー再生期限ＡＣｐ）を記録する（ステップＳ６４２）。このようにダミートランザクションＩＤ、ダミーコンテンツＩＤ、ダミーライセンス鍵Ｋｃ、ダミーアクセス制限情報ＡＣｍ、およびダミー再生期限ＡＣｐを記録することによってメモリカード１１０へチェックアウトされたライセンスを消去することができる。

【０３８７】その後、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、チェックアウト情報内のチェックアウト可能数を１だけ増やし、チェックアウト用トランザクションＩＤ、およびチェックアウト先のメモリカードの個別公開鍵ＫＰｍｃ４を削除してチェックアウト情報を更新する（ステップＳ６４３）。そして、ライセンス管理モジュール５１１は、トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍ、および再生期限ＡＣｐと更新したチェックアウト情報とを新たな機密情報ｎとして平文の機密ファイルを更新する（ステップＳ６４４）。その後、ライセンス管理モジュール５１１は、平文の機密ファイルをバインディング鍵Ｋｂによって暗号化してＨＤＤ５

３０に記録されている暗号化機密ファイル１６０を更新する（ステップＳ６４５）。

【０３８８】そうすると、ライセンス管理モジュール５１１は、メモリカード１００のデータ領域１４１５Ｃに記録されているチェックインしたライセンスに対応するコンテンツファイル（暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆ）とライセンス管理ファイルを削除する削除指示をＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して再生端末１００へ送信する（ステップＳ６４６）。再生端末１００のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介してコンテンツファイル（暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆ）とライセンス管理ファイルの削除指示を受信する（ステップＳ６４７）。そうすると、コントローラ１１０６は、（暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆ）とライセンス管理ファイルとを削除する指示をメモリカード１１０へ出力し、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４、およびバスＢＳ４を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆとライセンス管理ファイルとを削除する指示を受信し、バスＢＳ４を介してメモリ１４１５の暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆ）とライセンス管理ファイルとを削除する（ステップＳ６４８）。

【０３８９】パーソナルコンピュータ５０のライセンス管理モジュール５１１は、チェックインした楽曲を削除した再生リストを作成し（ステップＳ６４９）、再生リストと、再生リストの書換指示とをメモリカード１１０へ送信する（ステップＳ６５０）。メモリカード１１０のコントローラ１４２０は、再生端末１００を介して再生リストと書換指示とを受信し（ステップＳ６５１）、バスＢＳ４を介してメモリ１４１５の再生リストを受信した再生リストに書換え（ステップＳ６５２）、チェックイン動作が終了する（ステップＳ６５３）。

【０３９０】このように、暗号化コンテンツデータおよびライセンスをチェックアウトした相手先から暗号化コンテンツデータおよびライセンスを返却して貰うことによって、ライセンスの移動が禁止されるセキュリティレベルの低いライセンス管理モジュールからおよびライセンスが、セキュリティレベルの高いメモリカードへ貸出され、メモリカードにおいてセキュリティレベルの低いライセンス管理モジュールで取得したライセンスを送信できるため、再生端末においてセキュリティレベルの低いライセンス管理モジュールで取得したライセンスによって再生できる暗号化コンテンツデータを再生して楽しむことができる。

【０３９１】また、メモリカードへ貸出されたライセンスは、アクセス制限情報ＡＣｍによってメモリカードから他の記録機器（メモリカード、ライセンス管理デバイスおよびライセンス管理モジュール）に対して、チェックアウトしたライセンスが出力できないよう指定されているため、貸出したライセンスの流出することはない。貸出したライセンス管理モジュールに対してチェックイン（返却）することで、貸出したライセンスの権利が、貸出したライセンス管理モジュールに戻るようになっている。従って、著作者の意に反して複製ができることを許すものではなく、セキュリティレベルが低下する処理ではなく、著作権も保護されている。

【０３９２】［再生］次に、図３９および図４０を参照してメモリカード１１０に移動、およびチェックアウトされたコンテンツデータの再生端末１００（コンテンツ再生デバイスとも言う、以下同じ）における再生動作について説明する。なお、図２９における処理以前に、再生端末１０２のユーザは、再生リストファイルに従って、再生するコンテンツ（楽曲）を決定し、コンテンツファイルを特定し、ライセンス管理ファイルを取得していることを前提として説明する。

【０３９３】図３９を参照して、再生動作の開始とともに、再生端末１００のユーザから操作パネル１１０８を介して再生指示が再生端末１００にインプットされる（ステップＳ１０００）。そうすると、コントローラ１１０６は、バスＢＳ３を介して認証データ保持部１５００から認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａ２を読出し、メモリカードインタフェース１２００を介してメモリカード１１０へ認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａ２を出力する（ステップＳ１００２）。

【０３９４】そうすると、メモリカード１１０は、認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａ２を受理する（ステップＳ１００４）。そして、メモリカード１１０の復号処理部１４０８は、受理した認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａ２を、ＫＰａ保持部１４１４に保持されたレベル２認証鍵ＫＰａ２によって復号し（ステップＳ１００６）、コントローラ１４２０は復号処理部１４０８における復号処理結果から、認証処理を行なう。すなわち、認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａ２が正規の認証データであるか否かを判断する認証処理を行なう（ステップＳ１００８）。復号できなかった場合、ステップＳ１０４８へ移行し、再生動作は終了する。認証データが復号できた場合、コントローラ１４２０は、取得したクラス証明書Ｃｐ１がメモリ１４１５のＣＲＬ領域１４１５Ａから読出した禁止クラスリストＣＲＬに含まれるか否かを判断する（ステップＳ１０１０）。この場合、クラス証明書Ｃｐ１には識別番号が付与されており、コントローラ１４２０は、受理したクラス証明書Ｃｐ１の識別番号が禁止クラスリストＣＲＬの中に存在するか否かを判別する。クラス証明書Ｃｐ１が禁止クラスリストデータに含まれると判断されると、ステップＳ１０４８へ移行し、再生動作は終了する。

【０３９５】ステップＳ１０１０において、クラス証明書Ｃｐ１が禁止クラスリストデータＣＲＬに含まれていないと判断されると、メモリカード１１０のセッションキー発生部１４１８は、再生セッション用のセッションキーＫｓ２を発生させる（ステップＳ１０１２）。そして、暗号処理部１４１０は、セッションキー発生部１４１８からのセッションキーＫｓ２を、復号処理部１４０８で復号されたクラス公開暗号鍵ＫＰｐ１によって暗号化した｛Ｋｓ２｝Ｋｐ１をバスＢＳ３へ出力する（ステップＳ１０１４）。そうすると、コントローラ１４２０は、インタフェース１４２４および端子１４２６を介してメモリカードインタフェース１２００へ｛Ｋｓ２｝Ｋｐ１を出力する（ステップＳ１０１６）。再生端末１００のコントローラ１１０６は、メモリカードインタフェース１２００を介して｛Ｋｓ２｝Ｋｐ１を取得する。そして、Ｋｐ１保持部１５０２は、秘密復号鍵Ｋｐ１を復号処理部１５０４へ出力する。

【０３９６】復号処理部１５０４は、Ｋｐ１保持部１５０２から出力された、公開暗号鍵ＫＰｐ１と対になっている秘密復号鍵Ｋｐ１によって｛Ｋｓ２｝Ｋｐ１を復号し、セッションキーＫｓ２を暗号処理部１５０６へ出力する（ステップＳ１０１８）。そうすると、セッション鍵発生部１５０８は、再生セッション用のセッションキーＫｓ３を発生させ、セッションキーＫｓ３を暗号処理部１５０６へ出力する（ステップＳ１０２０）。暗号処理部１５０６は、セッションキー発生部１５０８からのセッションキーＫｓ３を復号処理部１５０４からのセッションキーＫｓ２によって暗号化して｛Ｋｓ３｝Ｋｓ２を出力し、コントローラ１１０６は、バスＢＳ３およびメモリカードインタフェース１２００を介して｛Ｋｓ３｝Ｋｓ２をメモリカード１１０へ出力する（ステップＳ１０２２）。

【０３９７】そうすると、メモリカード１１０の復号処理部１４１２は、端子１４２６、インタフェース１４２４、およびバスＢＳ４を介して｛Ｋｓ３｝Ｋｓ２を入力する（ステップＳ１０２４）。

【０３９８】図４０を参照して、復号処理部１４１２は、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２によって｛Ｋｓ３｝Ｋｓ２を復号して、再生端末１００で発生されたセッションキーＫｓ３を受理する（ステップＳ１０２６）。

【０３９９】再生端末のコントローラ１１０６は、メモリカード１１０から事前に取得した再生リクエスト由のライセンス管理ファイルからライセンスの格納されているエントリ番号を取得し、メモリカードインタフェース１２００を介してメモリカード１１０へ取得したエントリ番号を出力する（ステップＳ１０２７）。

【０４００】エントリ番号の入力に応じて、コントローラ１４２０は、アクセス制限情報ＡＣｍを確認する（ステップＳ１０２８）。ステップＳ１０２８においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報ＡＣｍを、具体的には、再生回数を確認することにより、確認することにより、既に再生不可の状態である場合には再生動作を終了し、アクセス制限情報の再生回数に回数制限がある場合にはアクセス制限情報ＡＣｍの再生回数を更新（１減ずる）した後に次のステップに進む（ステップＳ１０３０）。一方、アクセス制限情報ＡＣｍの再生回数によって再生回数が制限されていない場合においては、ステップＳ１０３０はスキップされ、アクセス制限情報ＡＣｍは更新されることなく処理が次のステップ（ステップＳ１０３２）に進行される。

【０４０１】ステップＳ１０２８において、当該再生動作において再生が可能であると判断された場合には、メモリ１４１５のライセンス領域１４１５Ｂに記録された再生リクエスト由のライセンス鍵Ｋｃおよび再生期間ＡＣｐがバスＢＳ４上に出力される（ステップＳ１０３２）。

【０４０２】得られたライセンス鍵Ｋｃと再生期限ＡＣｐは、切換スイッチ１４４６の接点Ｐｆを介して暗号化処理部１４０６に送られる。暗号化処理部１４０６は、切換スイッチ１４４２の接点Ｐｂを介して復号処理部１４１２より受けたセッションキーＫｓ３によって切換スイッチ１４４６を介して受けたライセンス鍵Ｋｃと再生期限ＡＣｐとを暗号化し、｛Ｋｃ／／ＡＣｐ｝Ｋｓ３をバスＢＳ４に出力する（ステップＳ１０３４）。

【０４０３】バスＢＳ４に出力された暗号化データは、インタフェース１４２４、端子１４２６、およびメモリカードインタフェース１２００を介して再生端末１００に送出される。

【０４０４】再生端末１００においては、メモリカードインタフェース１２００を介してバスＢＳ３に伝達される暗号化データ｛Ｋｃ／／ＡＣｐ｝Ｋｓ３を復号処理部１５１０によって復号処理を行ない、ライセンス鍵Ｋｃおよび再生期限ＡＣｐを受理する（ステップＳ１０３６）。復号処理部１５１０は、ライセンス鍵Ｋｃを復号処理部１５１６に伝達し、再生期限ＡＣｐをバスＢＳ３に出力する。

【０４０５】コントローラ１１０６は、バスＢＳ３を介して、再生期限ＡＣｐを受理して再生の可否の確認を行なう（ステップＳ１０４０）。

【０４０６】ステップＳ１０４０においては、再生期限ＡＣｐによって再生不可と判断される場合には、再生動作は終了される。

【０４０７】ステップＳ１０４０において再生可能と判断された場合、コントローラ１１０６は、メモリカードインタフェース１２００を介してメモリカード１１０のデータ領域１４１５Ｃにコンテンツファイルとして記録された暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを要求する。そうすると、メモリカード１１０のコントローラ１

４２０は、メモリ１４１５から暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを取得し、パスＢＳ４、インタフェース１４２４、および端子１４２６を介してメモリカードインタフェース１２００へ出力する（ステップＳ１０４２）。

【０４０８】再生端末１００のコントローラ１１０６は、メモリカードインタフェース１２００を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを取得し、パスＢＳ３を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを復号処理部１５１６へ与える。

【０４０９】そして、復号処理部１５１６は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを復号処理部１５１０から出力されたコンテンツ鍵Ｋｃによって復号してコンテンツデータＤａｔａを取得する（ステップＳ１０４４）。

【０４１０】そして、復号されたコンテンツデータＤｃは音楽再生部１５１８へ出力され、音楽再生部１５１８は、コンテンツデータを再生し、ＤＡ変換器１５１９はディジタル信号をアナログ信号に変換して端子１５３０へ出力する。そして、音楽データは端子１５３０から外部出力装置を介してヘッドホン１３０へ出力されて再生される（ステップＳ１０４６）。これによって再生動作が終了する。

【０４１１】上記においては、メモリカード１１０に記録された暗号化コンテンツデータを再生端末１００によって再生する場合について説明したが、パーソナルコンピュータ５０，８０に、図７に示すコンテンツ再生デバイス１５５０を内蔵することによってライセンス管理モジュール５１１およびライセンス管理デバイス５２０によって受信された暗号化コンテンツデータを再生することが可能である。なお、ライセンス管理モジュール５１１によって取得された暗号化コンテンツデータをコンテンツ再生デバイス１５５０により再生する場合、ライセンス管理モジュール５１１は、ライセンス管理デバイス５２０に格納されたバインディング鍵Ｋｂを取得し、ＨＤＤ５３０に記録された暗号化機密ファイル１６０をバインディング鍵Ｋｂによって復号し、平文の機密ファイルからライセンスを読出してコンテンツ再生デバイス１５５０へ与える。

【０４１２】また、パーソナルコンピュータ５０，８０に暗号化コンテンツデータを再生するソフトウエアに従って機能する再生部を内蔵することによって、ライセンス管理モジュール５１１が取得した暗号化コンテンツデータをソフトウエアにより再生することが可能である。この場合も、ライセンス管理モジュール５１１は、ライセンス管理デバイス５２０に格納されたバインディング鍵Ｋｂを取得し、ＨＤＤ５３０に記録された暗号化機密ファイル１６０をバインディング鍵Ｋｂによって復号し、平文の機密ファイルからライセンスを読出してコンテンツ再生デバイス１５５０へ与える。コンテンツ再生デバイス１５５０を用いたハード的に機密性を持つ再生（レベル２）に比べて、ソフトウエアによる再生は、ソフト的に機密性を持つ再生（レベル１）であるためセキュリティレベルが低い処理である。ゆえに、ライセンス管理デバイス５２０にて保持されるライセンスは、このソフトウェアによる再生では使用できない。

【０４１３】［移動２］図１に示すデータ配信システムにおいて、パーソナルコンピュータ５０のライセンス管理モジュール５１１が取得した暗号化コンテンツデータおよびライセンスをパーソナルコンピュータ８０へ移動する動作について説明する。なお、この移動を［移動２］という。

【０４１４】図４１～図４８は、ライセンス管理モジュール５１１が取得した暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ８０への移動を説明するための第１～第８のフローチャートである。なお、図４１における処理以前に、パーソナルコンピュータ５０のユーザは、コンテンツリストファイルに従って、移動するコンテンツを決定し、ＨＤＤ５３０およびメモカード１１０のコンテンツファイルおよびライセンス管理ファイルが特定していることを前提に説明する。また、受信側のパーソナルコンピュータ８０におけるライセンス管理モジュールのクラスを識別する自然数ｗはｗ＝５であり、ライセンス管理モジュールを識別する自然数ｙはｙ＝５とする。

【０４１５】図４１を参照して、パーソナルコンピュータ５０のキーボード５６０を介してパーソナルコンピュータ５０のライセンス管理モジュール５１１によって取得されたライセンスの移動リクエストが入力されると（ステップＳ８００）、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、バインディング鍵取得処理を行う。図４１のステップＳ８０１から図４２のステップＳ８１５の一連の処理がバインディング鍵取得処理であり、配信２のフローチャートにおける図２０のステップＳ２７０から図２１のステップＳ２８４の一連の処理と同じである。ゆえに、説明を省略する。

【０４１６】バインディングライセンスを取得すると、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、パスＢＳ２を介してＨＤＤ５３０から暗号化機密ファイル１６０を取得し、その取得した暗号化機密ファイル１６０をバインディング鍵Ｋｂによって復号して平文の機密ファイルを取得する（ステップＳ８１６）。その後、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、ライセンス管理ファイルに記録された機密情報番号ｎに対応する機密ファイル内の機密情報ｎ（トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍ、再生期限ＡＣｐ、およびチェックアウト情報）を取得する（ステップＳ８１７）。

【０４１７】そうすると、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、取得したアクセ

ス制限情報ＡＣｍに基づいて暗号化コンテンツデータの移動および複製が可能か否かを確認する（ステップＳ５１８）、つまり、ライセンス管理モジュール５１１は、取得したアクセス制限情報ＡＣｍの再生回数、移動複製フラグに基づいて、パーソナルコンピュータ８０へ移動しようとするライセンスがアクセス制限情報ＡＣｍによって暗号化コンテンツデータの移動および複製ができないライセンスになっていないか否かを確認する。

【０４１８】ステップＳ８１８において、暗号化コンテンツデータの移動および複製が禁止されていた場合、ステップＳ９０３へ移行し、移動動作は終了する。ステップＳ８１８において、暗号化コンテンツデータの移動および複製が禁止されていない場合、ステップＳ８１９へ移行する。そして、ライセンス管理モジュール５１１は、取得したチェックアウト情報に基づいてチェックアウトが可能か否かを確認する（ステップＳ８１９）。ステップＳ８１９において、チェックアウトが不可能であれば、チェックアウトが禁止されているので、ステップＳ９０３へ移行し、チェックアウト動作は終了する。ステップＳ８１９において、チェックアウト可能であれば、新たなバインディング鍵を、ライセンス管理デバイス５２０に格納できるかを確認するためにデバイス確認処理を行なうデバイス確認処理において、ライセンス管理デバイス５２０が認証できない、あるいは、禁止クラスリストＣＲＬにより、新たなバインディング鍵が記録できない場合には、現状を維持するために、処理は中断する。図４２のステップＳ８２１から図４３のステップＳ８３３の一連の処理がデバイス確認処理であり、初期化のフローチャートにおける図１０のステップＳ１６から図１１のステップＳ４２の一連の処理と同じである。ゆえに、説明を省略する。

【０４１９】デバイス確認処理が終了すると、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、認証データの送信要求を通信ケーブル９０を介してパーソナルコンピュータ８０へ送信する（ステップＳ８３４）。そうすると、パーソナルコンピュータ８０のライセンス管理モジュールは、認証データの送信要求を受信する（ステップＳ８３５）。

【０４２０】パーソナルコンピュータ８０のライセンス管理モジュールは、認証データの送信要求を受信すると、認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰａ１をパーソナルコンピュータ５０へ送信する（ステップＳ８３６）。パーソナルコンピュータ５０のライセンス管理モジュール５１１は、端子５８０およびＵＳＢインタフェース５５０を介して認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰａ１を受信し（ステップＳ８３７）、その受信した認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰａ１をレベル１認証鍵ＫＰａ１によって復号する（ステップＳ８３８）。

【０４２１】図４４を参照して、ライセンス管理モジュール５１１は、復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード１１０が正規のメモリカードからのクラス公開暗号鍵ＫＰｍ５とクラス証明書Ｃｍ５とを保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ８３９）。正当な認証データであると判断された場合、ライセンス管理モジュール５１１は、公開暗号鍵ＫＰｍ３および証明書Ｃｍ３を承認し、受理する。そして、次の処理（ステップＳ８４０）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵ＫＰｍ５およびクラス証明書Ｃｍ５を受理しないで処理を終了する（ステップＳ９０３）。認証の結果、正規のメモリカードであることが認識されると、ライセンス管理モジュール５１１は、次に、メモリカード１１０のクラス証明書Ｃｍ３が禁止クラスリストＣＲＬにリストアップされているかどうかをＨＤＤ５３０に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで移動動作を終了する（ステップＳ９０３）。一方、メモリカード１１０のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップＳ８４０）。

【０４２２】認証の結果、正当な認証データを持つメモリカードを備える再生端末からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されるとライセンス管理モジュール５１１は、移動用のセッションキーＫｓ２ｄを生成する（ステップＳ８４１）。そして、ライセンス管理モジュール５１１は、生成したセッションキーＫｓ２ｄをパーソナルコンピュータ８０から受信したクラス公開暗号鍵ＫＰｍ５によって暗号化し、暗号化データ｛Ｋｓ２ｄ｝Ｋｍ５を生成し（ステップＳ８４２）、暗号化データ｛Ｋｓ２ｄ｝Ｋｍ５にトランザクションＩＤを追加したトランザクションＩＤ／／｛Ｋｓ２ｄ｝Ｋｍ５を通信ケーブル９０を介してパーソナルコンピュータ８０へ送信する（ステップＳ８４３）。パーソナルコンピュータ８０のライセンス管理モジュールは、トランザクションＩＤ／／｛Ｋｓ２ｄ｝Ｋｍ５を受信する（ステップＳ８４４）。そして、パーソナルコンピュータ８０のライセンス管理モジュールは、クラス秘密復号鍵Ｋｍ３によって｛Ｋｓ２ｄ｝Ｋｍ５を復号してセッションキーＫｓ２ｄを受理する（ステップＳ８４５）。そして、パーソナルコンピュータ８０のライセンス管理モジュールは、セッションキーＫｓ２ｅを生成し（ステップＳ８４６）、ＨＤＤから禁止クラスリストＣＲＬの更新日時ＣＲＬｄａｔｅを取得する（ステップＳ８４７）。

【０４２３】そして、パーソナルコンピュータ８０のライセンス管理モジュールは、セッションキーＫｓ２ｅ、個別公開暗号鍵ＫＰｍｃ５および禁止クラスリストＣＲＬｄａｔｅをセッションキーＫｓ２ｄによって暗号化

し、暗号化データ｛Ｋｓ２ｅ／／ＫＰｍｃ５／／ＣＲＬｄａｔｅ｝Ｋｓ２ｄを生成し、暗号化データ｛Ｋｓ２ｅ／／ＫＰｍｃ５／／ＣＲＬｄａｔｅ｝Ｋｓ２ｄを通信ケーブル９０を介してパーソナルコンピュータ５０へ送信する（ステップＳ８４８）。

【０４２４】パーソナルコンピュータ５０のライセンス管理モジュール５１１は、端子５８０およびＵＳＢインタフェース５５０を介して暗号化データ｛Ｋｓ２ｃ／／ＫＰｍｃ５／／ＣＲＬｄａｔｅ｝Ｋｓ２ｄを受信し（ステップＳ８４９）、その受信した暗号化データ｛Ｋｓ２ｅ／／ＫＰｍｃ５／／ＣＲＬｄａｔｅ｝Ｋｓ２ｄをセッションキーＫｓ２ｄによって復号し、セッションキーＫｓ２ｅ、個別公開暗号鍵ＫＰｍｃ５および更新日時ＣＲＬｄａｔｅを受理する（ステップＳ８５０）。そして、ライセンス管理モジュール５１１は、トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍ、および再生期限ＡＣｐをパーソナルコンピュータ８０に固有の個別公開暗号鍵ＫＰｍｃ５によって暗号化して暗号化データ｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ５を生成する（ステップＳ８５１）。

【０４２５】図４５を参照して、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、パーソナルコンピュータ８０のライセンス管理モジュールから送信された禁止クラスリストの更新日時ＣＲＬｄａｔｅに基づいてパーソナルコンピュータ８０のライセンス管理モジュールが管理する禁止クラスリストと自身の管理する禁止クラスリストのどちらが新しいか判断し、自身の管理する禁止クラスリストＣＲＬが古いと判断されたとき、ステップＳ８５３へ移行する。また、逆に、自身の管理する禁止クラスリストＣＲＬの方が新しいと判断されたときはステップＳ８５６へ移行する（ステップＳ８５２）。

【０４２６】自身の管理する禁止クラスリストＣＲＬが古いと判断されたとき、ライセンス管理モジュール５１１は、暗号化データ｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ５をライセンス管理モジュール５１１において発生されたセッションキーＫｓ２ｅによって暗号化を行い、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ５｝Ｋｓ２ｅを通信ケーブル９０を介してパーソナルコンピュータ８０へ送信する（ステップＳ８５３）。

【０４２７】そして、パーソナルコンピュータ８０のライセンス管理モジュールは、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ５｝Ｋｓ２ｅを受信し（ステップＳ８５４）、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ５｝Ｋｓ２ｅをセッションキーＫｓ２ｅによって復号し、｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ５を受理する（ステップＳ８５５）。その後、ステップＳ８６１へ移行する。

【０４２８】一方、ステップＳ８５２において、自身の管理する禁止クラスリストＣＲＬが新しいと判断されると、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、ＨＤＤ５３０から禁止クラスリストＣＲＬを取得する（ステップＳ８５６）。そして、ライセンス管理モジュール５１１は、禁止クラスリストＣＲＬと暗号化データ｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ５とを受けて、セッションキーＫｓ２ｅによって暗号化して暗号化データ｛ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ５｝Ｋｓ２ｅを通信ケーブル９０を介してパーソナルコンピュータ８０に送信する（ステップＳ８５７）。

【０４２９】パーソナルコンピュータ８０は、送信された暗号化データ｛ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ５｝Ｋｓ２ｅを受信し（ステップＳ８５８）、ライセンス管理モジュールは、セッションキーＫｓ２ｅを用いて受信データを復号してＣＲＬと暗号化データ｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ５と受理する（ステップＳ８５９）。

【０４３０】パーソナルコンピュータ８０のライセンス管理モジュールは、ＨＤＤに記録された禁止クラスリストＣＲＬを受理したＣＲＬによって書換える（ステップＳ８６０）。

【０４３１】ステップＳ８５３，Ｓ８５４，Ｓ８５５は、パーソナルコンピュータ８０から送られてきた禁止クラスリストの更新日時ＣＲＬｄａｔｅによって、受信側のパーソナルコンピュータ８０の保持する禁止クラスリストＣＲＬが送信側のパーソナルコンピュータ５０の保持する禁止クラスリストＣＲＬの方が新しい場合のライセンス鍵Ｋｃ等のパーソナルコンピュータ８０への移動動作であり、ステップＳ８５４，Ｓ８５５，Ｓ８５６，Ｓ８５７，Ｓ８６０は、受信側のパーソナルコンピュータ８０の保持する禁止クラスリストＣＲＬが送信側のパーソナルコンピュータ５０の保持する禁止クラスリストＣＲＬの方が古い場合のライセンス鍵Ｋｃ等のパーソナルコンピュータ８０への移動動作である。

【０４３２】ステップＳ８５５またはステップＳ８６０の後、パーソナルコンピュータ８０のライセンス管理モジュールは、暗号化データ｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ５は、個別秘密復号鍵Ｋｍｃ５によって復号し、ライセンス（ライセンス鍵Ｋｃ、トランザクションＩＤ、コンテンツＩＤ、アクセス制限情報ＡＣｍおよび再生期限ＡＣｐ）を受理する（ステップＳ８６１）。そして、ライ

センス管理モジュールは、受理したアクセス制限情報ＡＣｍによって再生回数が制限されているか否かを判別し、再生回数が制限されていないときステップＳ８６３へ移行し、再生回数が制限されているときステップＳ８６４へ移行する（ステップＳ８６２）。そして、再生回数が制限されていなとき、ライセンス管理モジュールは、パーソナルコンピュータ５０から受信した暗号化コンテンツおよびライセンスを他の装置へ貸出すためのチェックアウト可能数を含むチェックアウト情報を生成する（ステップＳ８６３）。この場合、チェックアウトの初期値は「３」に設定される。また、再生回数が制限されているとき、ライセンス管理モジュールは、暗号化コンテンツデータを他の装置へ貸出すためのチェックアウト可能数を「０」に設定してチェックアウト情報を生成する（ステップＳ８６４）。その後、図４６のステップＳ８８０へ移行する。

【０４３３】ステップＳ８５３またはステップＳ８５７の後、パーソナルコンピュータ５０がライセンスをパーソナルコンピュータ８０へ移動するのと並行してパーソナルコンピュータ５０が保持するバインディングライセンスの書換え動作が行なわれる。ステップＳ８５３またはステップＳ８５７の後、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、アクセス制限情報ＡＣｍに基づいてライセンスの複製が可能か否かを判別する（ステップＳ８６５）。そして、ライセンスの複製が可能な場合、図４８のステップＳ８９８へ以降し、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆをパーソナルコンピュータ８０へ送信する。ステップＳ８６５において、ライセンスのアクセス制限情報ＡＣｍの移動復号フラグによって移動のみ可の場合、ライセンス管理モジュール５１１は、ＨＤＤ５３０に記録された移動させたライセンスに関するコンテンツリストファイル１５０のライセンス管理ファイル１５２ｎを読出し、ライセンス管理ファイルに記録された機密情報番号ｎを、ライセンス無に変更してライセンス管理ファイル１５２ｎを更新し（ステップＳ８６６）、最初の生成したバインディング鍵Ｋｂと異なる新たにバインディング鍵Ｋｂｂを生成する（ステップＳ８６７）。そして、ライセンス管理モジュール５１１は、平文の機密ファイル内の機密情報ｎを削除し、機密ファイルを新たに生成したバインディング鍵Ｋｂｂによって暗号化してＨＤＤ５３０内の暗号化機密ファイル１６０を更新する（ステップＳ８６８）。

【０４３４】図４６を参照して、ライセンス管理モジュール５１１は、新たに生成したバインディング鍵Ｋｂｂをライセンス管理デバイス５２０に格納するためにステップＳ８６９からステップＳ８７９のバインディング鍵登録処理を行う。初期化のフローチャートにおける図１１のステップＳ４４から図１２のステップＳ６６の一連の処理と同じ処理であり、バインディング鍵Ｋｂが、新たなバインディング鍵Ｋｂｂにセッション鍵Ｋｓ２ｂがセッション鍵Ｋｓ２ｃに変更されているのみである。ゆえに、説明を省略する。

【０４３５】新たなバインディング鍵Ｋｂｂの登録が終了すると、図４８のステップＳ８９８へ移行する。

【０４３６】図４７を参照して、図４５のステップＳ８６１またはステップＳ８６２の後、パーソナルコンピュータ８０においては、内蔵するライセンス管理モジュールからのバインディング鍵Ｋｂ２の取得、すなわちバインディング鍵の取得処理を行う。パーソナルコンピュータ８０においても、パーソナルコンピュータ５０と同じであり、ステップＳ８７８から図４８ステップＳ８９３に至る一連の処理がバインディング鍵取得処理であり、配信２のフローチャートにおける図２０のステップＳ２７０から図２１のステップＳ２８４に至る一連の処理と同じであり、取得するバインディングライセンス｛トランザクションＩＤｂ２，コンテンツＩＤｂ２，バインディング鍵Ｋｂ２，および制御情報ＡＣｍｂ２，ＡＣｐｂ２｝に、また、セッション鍵Ｋｓ２ａとＫｓ２ｂは、それぞれＫｓ２ｇとＫｓ２ｆに変更されているのみである。ゆえに、説明を省略する。

【０４３７】バインディング鍵Ｋｂ２を取得すると、パーソナルコンピュータ８０のライセンス管理モジュールは、パスＢＳ２を介してＨＤＤ５３０から暗号化機密ファイル１６０を取得し、その取得した暗号化機密ファイル１６０をバインディング鍵Ｋｂ２によって復号して平文の機密ファイルを取得する（ステップＳ８９５）。その後、ライセンス管理モジュールは、パーソナルコンピュータ５０から受信したライセンス（トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍ、再生期限ＡＣｐ）およびチェックアウト情報を新たな機密情報ｎ２として平文の機密ファイルに追記する（ステップＳ８９６）。そして、ライセンス管理モジュールは、平文の機密ファイルをバインディング鍵Ｋｂ２によって暗号化してＨＤＤに記録されている暗号化機密ファイル１６０を更新する（ステップＳ８９７）。

【０４３８】そうすると、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、図４５のステップＳ８６８およびステップＳ８９７が共に終了すると、ＨＤＤ５３０に記録されているコンテンツファイル（暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆ）を読出し、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆとを通信ケーブル９０を介してパーソナルコンピュータ８０へ送信する（ステップＳ８９８）。

【０４３９】パーソナルコンピュータ８０のライセンス管理モジュールは、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆとを受信し、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆとを受理

する（ステップＳ８９９）。そして、ライセンス管理モジュールは、受理した暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆとをバスＢＳ２をコンテンツファイルとして介してＨＤＤに記録する（ステップＳ９００）。また、ライセンス管理モジュールは、機密情報番号ｎ２、トランザクションＩＤおよびコンテンツＩＤを含む、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆとを記録したコンテンツファイルに対するライセンス管理ファイルを作成してＨＤＤに記録する（ステップＳ９０１）。そして、ライセンス管理モジュールは、ＨＤＤに記録されているコンテンツリストファイルのコンテンツファイルに受理したコンテンツの名称を追記し（ステップＳ９０２）、移動動作が終了する（ステップＳ９０３）。

【０４４０】このように、パーソナルコンピュータ５０のライセンス管理モジュール５１１が取得した暗号化コンテンツデータのライセンスをバインディング鍵Ｋｂによって管理することによって、パーソナルコンピュータ５０からパーソナルコンピュータ８０へ暗号化コンテンツデータおよびライセンスを移動することができる。

【０４４１】実施の形態１によれば、パーソナルコンピュータに内蔵されたライセンス管理モジュールがソフトウエアによって取得した暗号化コンテンツデータのライセンスをライセンス管理デバイスによりハード的に管理されるバインディング鍵によって管理するので、ライセンス管理デバイスによって取得された暗号化コンテンツデータのライセンスと同じように「移動」という概念によって他のパーソナルコンピュータへ暗号化コンテンツデータおよびライセンスを送信することが可能である。

【０４４２】【実施の形態２】図４９を参照して、ライセンス管理モジュール５１１によって取得された暗号化コンテンツデータのライセンスの実施の形態２における管理方法について説明する。

【０４４３】コンテンツリストファイル１５０の構成は実施の形態１における構成と同じである。ＨＤＤ５３０には、暗号化機密ファイル１６０が記録されており、これには、ライセンス管理デバイス５２０に格納されたトランザクションＩＤｂ、コンテンツＩＤｂ、およびバインディング鍵Ｋｂと同じものが格納されている。そして、暗号化機密ファイル１６０は、パーソナルコンピュータ５０のＣＰＵのシリアル番号等に依存した、パーソナルコンピュータ５０から持ち出し不可能となるように独自の暗号化が施されている。また、ライセンス管理ファイル１５２２，・・，１５２ｎの内、ライセンス管理モジュール５１１によって取得されたライセンスに対するライセンス管理ファイルでは、ライセンス管理ファイル１５２２および１５２ｎがそれに当たる。ライセンスおよびチェックアウト情報を含む機密情報を、暗号化機密ファイルと同様に暗号化した暗号化機密情報と、ライセンスに関する平文情報とを含んでいる。バインディングライセンスは格納するライセンス管理デバイス５２０のエントリ番号「０」に常に格納する。

【０４４４】また、ライセンス管理デバイスにライセンスを格納したライセンスに対するライセンス管理ファイル、ライセンス管理ファイル１５２１および１５２ｎがこれに当たる、暗号化機密情報に換えて、ライセンス管理デバイスのライセンス領域１４１５Ｂのライセンスするエントリを特定するエントリ番号化記録されている。他のファイルおよびライセンス領域１４１５Ｂの構成については、実施の形態１の図２５と同じであるので説明を省略する。

【０４４５】ライセンス管理ファイル１５２２，・・，１５２ｎからライセンスを取出すときは、ライセンス管理ファイル１５２２，・・，１５２ｎが暗号化機密情報含んでいれば、ライセンス管理デバイス５２０にエントリ番号「０」を送信してライセンス管理デバイス５２０からバインディング鍵Ｋｂを取得し、その取得したバインディング鍵Ｋｂが暗号化機密ファイル１６０に格納されたバインディング鍵Ｋｂに一致することを確認する。一致していれば、暗号化機密情報を復号して、ライセンスおよびチェックアウト情報を取得する。一致しなければライセンスの取得は禁止されるので処理を中止する。一方、エントリ番号が含まれる場合には、ライセンス管理デバイス５２０に処理を任せる。さらには、ライセンス無の場合には、ライセンスは存在しないので処理を中止する。したがって、この実施の形態２においては、セキュリティレベルが低い（レベル１）のライセンスに対する全ての処理において、ライセンス管理デバイス５２０に格納されたバインディング鍵Ｋｂと暗号化機密ファイル１６０に格納されたバインディング鍵Ｋｂとが一致しなければライセンス管理ファイル１５２２，・・，１５２ｎから暗号化のコンテンツデータのライセンスを取出すことができないように運用する。

【０４４６】その結果、この実施の形態２においても、ライセンス管理モジュール５１１によって取得された暗号化コンテンツデータのライセンスは、バインディング鍵Ｋｂによって管理することができ、実施の形態１で説明したのと同じようにパーソナルコンピュータ５０からパーソナルコンピュータ８０への暗号化コンテンツデータおよびライセンスの移動が可能となる。

【０４４７】［初期化］図５０～図５２は、実施の形態２における暗号化機密ファイル１６０の初期化を説明するための第１～第３のフローチャートである。図５０～図５２に示すフローチャートは、図１０～図１２にフローチャートのステップＳ６６をステップＳ６６ａに代えたものであり、それ以外は図１０～図１２のフローチャートと同じである。したがって、図５２を参照して、ステップＳ６４の後、ライセンス管理モジュール５１１は、トランザクションＩＤｂ、コンテンツＩＤｂおよびバインディング鍵Ｋｂを平文の機密ファイルに格納し、

平文の機密ファイルに独自の暗号化を施して暗号化機密ファイル１６０を作成し、その作成した暗号化機密ファイル１６０をＨＤＤ５３０に記録する（ステップＳ６６ａ）。そして、初期化の動作は終了する（ステップＳ６８）。

【０４４８】［配信２］図５３～図５６には、実施の形態２において、ライセンス管理モジュール５１１から配信サーバ１０から暗号化コンテンツデータおよびライセンスを受信するときの動作を説明するための第１～第４のフローチャートである。図５３～図５６に示すフローチャートは、図１７～図２１に示すフローチャートのステップＳ２６６，Ｓ２６８とステップＳ２８８との間のステップをステップＳ２８７ａ～Ｓ２８７ａに代えたものであり、その他は、図１７～図２１に示すフローチャートと同じである。図５６を参照して、ステップＳ２６６，Ｓ２６８において、チェックアウト情報が生成された後、ライセンス管理モジュール５１１は、受理したライセンス（トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍおよび再生期限ＡＣｐ）とチェックアウト情報とバインディング情報とに独自の暗号化を施して暗号化機密情報を生成する（ステップＳ２８６ａ）。そして、ライセンス管理モジュール５１１は、生成した暗号化機密情報、トランザクションＩＤ、およびコンテンツＩＤを含むライセンス管理ファイルを作成してＨＤＤ５３０に記録する（ステップＳ２８７ａ）。その後、ステップＳ２８８へ移行して上述した各ステップが実行されて暗号化コンテンツデータおよびライセンスの配信動作が終了する。

【０４４９】［リッピング］図５７および図５８は、実施の形態２において、ライセンス管理モジュール５１１が音楽ＣＤから暗号化コンテンツデータおよびライセンスを取得するリッピングの動作を説明するための第１および第２のフローチャートである。図５７および図５８に示すフローチャートは、図２２～図２４に示すフローチャートのステップＳ７０８とステップＳ７２５との間のステップをステップをステップＳ７２０ａ～ステップＳ７２４ａに代えたものであり、それ以外は、図２２～図２４に示すフローチャートと同じである。図５８を参照して、ステップＳ７０８の後、ライセンス管理モジュール５１１は、受理したライセンス（トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍおよび再生期限ＡＣｐ）とチェックアウト情報とバインディング情報とに独自の暗号化を施して暗号化機密情報を生成する（ステップＳ７２３ａ）。そして、ライセンス管理モジュール５１１は、生成した暗号化機密情報、トランザクションＩＤ、およびコンテンツＩＤを含むライセンス管理ファイルを作成してＨＤＤ５３０に記録する（ステップＳ７２４ａ）。その後、ステップＳ７２５へ移行して上述した各ステップが実行されて暗号化コンテンツデータおよびライセンスのリッピングの動作が終了する。

【０４５０】［チェックアウト］図５９～図６３は、実施の形態２において、ライセンス管理モジュール５１１が取得した暗号化コンテンツデータおよびライセンスを再生端末１００に装着されたメモリカード１１０へチェックアウトする動作を説明するための第１～第５のフローチャートである。図５９～図６３に示すフローチャートは、図３０～図３４に示すフローチャートのステップＳ５１６，Ｓ５１７をステップＳ５１６ａ，Ｓ５１６ｂ，Ｓ５１７ａに代え、ステップＳ５５２，Ｓ５５３をステップＳ５５２ａ，５５３ａに代えたものであり、それ以外は、図３０～図３４に示すフローチャートと同じである。図６０を参照して、ステップＳ５１５の後、ライセンス管理モジュール５１１は、ＨＤＤ５３０に記録されている暗号化機密ファイル１６０を取得し、復号して格納されているバインディング鍵Ｋｂを取得する（ステップＳ５１６ａ）。そして、ライセンス管理モジュール５１１は、ライセンス管理デバイス５２０から取得したバインディング鍵Ｋｂが暗号化機密ファイル１６０から取得したバインディング鍵Ｋｂに一致するか否かを判別し、２つのバインディング鍵Ｋｂが相互に一致しないとき、ステップＳ５６４へ移行してチェックアウトの動作は終了する。２つのバインディング鍵Ｋｂが相互に一致するときは、次のステップＳ５１７ａへ移行する（ステップＳ５１６ｂ）。

【０４５１】ライセンス管理デバイス５２０から取得したバインディング鍵Ｋｂが暗号化機密ファイル１６０から取得したバインディング鍵Ｋｂに一致したとき、ライセンス管理ファイルから暗号化機密情報を取得して、復号したライセンス（ライセンス鍵Ｋｃ、トランザクションＩＤ、コンテンツＩＤ、アクセス制限情報ＡＣｍおよび再生回数ＡＣｐ）を得る（ステップＳ５１７ａ）。そして、次のステップＳ５１１８へ移行する図６３を参照して、ステップＳ５５１の後、ライセンス管理モジュール５１１は、更新したチェックアウト情報を反映させた機密情報に独自の暗号化を施して暗号化機密情報を生成し（ステップＳ５５２ａ）、暗号化機密情報を含むライセンス管理ファイルを更新する（ステップＳ５５３ａ）。その後、ステップＳ５５４へ移行して上述した各ステップが実行されて暗号化コンテンツデータおよびライセンスのチェックアウトの動作が終了する。

【０４５２】このように、ライセンス管理デバイス５２０に格納されたバインディング鍵が暗号化機密ファイル１６０に格納されたバインディング鍵に一致する場合だけ、ライセンス管理モジュールは、ライセンス管理ファイルから暗号化コンテンツデータのライセンスを取得する。したがって、実施の形態２においても、バインディング鍵によって暗号化コンテンツデータのライセンスを実質的に管理する。

【０４５３】［チェックイン］図６４～図６７は、実施

の形態２において、ライセンス管理モジュール５１１が再生端末１００に装着されたメモリカード１１０へチェックアウトした暗号化コンテンツデータおよびライセンスをチェックインする動作を説明するための第１～第４のフローチャートである。図６４～図６７に示すフローチャートは、図３５～図３８に示すフローチャートのステップＳ６１６，Ｓ６１７をステップＳ６１６ａ，６１６ｂ，６１７ａに代え、ステップＳ６４３，Ｓ６４４をステップＳ６４３ａ，６４４ａに代えたものであり、それ以外は、図３５～図３８に示すフローチャートと同じである。

【０４５４】図６５を参照して、ステップＳ６１５の後、ライセンス管理モジュール５１１は、ＨＤＤ５３０に記録されている暗号化機密ファイル１６０を取得し、復号して格納されているバインディング鍵Ｋｂを取得する（ステップＳ６１６ａ）。そして、ライセンス管理モジュール５１１は、ライセンス管理デバイス５２０から取得したバインディング鍵Ｋｂが暗号化機密ファイル１６０から取得したバインディング鍵Ｋｂに一致するか否かを判別し、２つのバインディング鍵Ｋｂが相互に一致しないとき、ステップＳ６５３へ移行してチェックインの動作は終了する。２つのバインディング鍵Ｋｂが相互に一致するときは、次のステップＳ６１８へ移行する（ステップＳ６１６ｂ）。

【０４５５】ライセンス管理デバイス５２０から取得したバインディング鍵Ｋｂが暗号化機密ファイル１６０から取得したバインディング鍵Ｋｂに一致したとき、ライセンス管理ファイルから暗号化機密情報を取得して、復号したライセンス（ライセンス鍵Ｋｃ、トランザクションＩＤ、コンテンツＩＤ、アクセス制限情報ＡＣｍおよび再生回数ＡＣｐ）を得る（ステップ６１７ａ）。そして、次のステップＳ５１１８へ移行する。

【０４５６】図６７を参照して、ステップＳ６４２の後、ライセンス管理モジュール５１１は、更新したチェックアウト情報を反映させた機密情報に独自の暗号化を施して暗号化機密情報を生成し（ステップＳ６４４ａ）、暗号化機密情報を含むライセンス管理ファイルを更新する（ステップＳ６４５ａ）。その後、ステップＳ６４６へ移行して上述した各ステップが実行されて暗号化コンテンツデータおよびライセンスのチェックインの動作が終了する。

【０４５７】［移動２］図６８～図７４は、実施の形態２において、ライセンス管理モジュール５１１が受信した暗号化コンテンツデータおよびライセンスをパーソナルコンピュータ５０からパーソナルコンピュータ８０へ移動する動作を説明するための第１～第７のフローチャートである。図６８～図７４に示すフローチャートは、図３９～図４６に示すフローチャートのステップＳ８００とステップＳ８０１との間にステップＳ８００ａ～ステップＳ８００ｃを挿入し、ステップＳ８１５とステップＳ８２０との間のステップをステップＳ８１６ａ，８１７ａに代え、ステップＳ８６７をステップＳ８６７ａとステップＳ８６７ｂに代え、ステップＳ８６２，Ｓ８６３とステップＳ８９７との間のステップをステップＳ８９５ａ～８９６ａに代えたものであり、それ以外は、図３９～図４６に示すフローチャートと同じである。

【０４５８】図６８を参照して、ライセンス管理モジュール５１１は、ステップＳ８００の後、ライセンス管理モジュール５１１は、ライセンス管理ファイルの暗号化機密情報を復号して機密情報（トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍ、再生期限ＡＣｐ、チェックアウト情報を取得する（ステップＳ８００ａ）。そして、ライセンス管理モジュール５１１は、ステップＳ８００ａにおいて取得したＡＣｍに基づいて暗号化コンテンツデータおよびライセンスの移動および複製が可能か否かを判別する。そして、ライセンス管理モジュール５１１は、暗号化コンテンツデータおよびライセンスの移動および複製が禁止されているとき、ステップＳ９０３へ移行して移動動作は終了し、移動および複製が禁止されていないときステップＳ８００ｃへ移行する（ステップＳ８００ｂ）。

【０４５９】ライセンス管理モジュール５１１は、暗号化コンテンツデータおよびライセンスの移動および複製が可能であるとき、チェックアウト情報に基づいてチェックアウト可能か否かを判別し、不可能なときステップＳ９０３へ移行して移動動作は終了し、チェックアウト可能なときステップＳ８０１へ移行する。

【０４６０】図６９を参照して、ステップＳ８１５の後、ライセンス管理モジュール５１１は、ＨＤＤ５３０に記録されている暗号化機密ファイル１６０を取得し、復号して格納されているバインディング鍵Ｋｂを取得する（ステップＳ８１６ａ）。そして、ライセンス管理モジュール５１１は、ライセンス管理デバイス５２０から取得したバインディング鍵Ｋｈが暗号化機密ファイル１６０から取得したバインディング鍵Ｋｂに一致するか否かを判別し、２つのバインディング鍵Ｋｂが相互に一致しないとき、ステップＳ９０３へ移行して移動の動作は終了する。２つのバインディング鍵Ｋｂが相互に一致するときは、次のステップＳ８２０へ移行する（ステップＳ８１７ａ）。

【０４６１】図７２を参照して、ステップＳ８６７の後、ライセンス管理モジュール５１１は、平分の機密ファイルに格納されているバインディング鍵Ｋｂをバインディング鍵Ｋｂｂに書換へ（ステップＳ８６８ａ）、独自の暗号化を施した暗号化機密ファイルを生成して、ＨＤＤ５３０の暗号化機密ファイルと書き換える（ステップＳ８６８ｂ）。次いで、図７３のステップＳ８６９へ移行する。

【０４６２】図７４を参照してステップＳ８６２，Ｓ８６３において、チェックアウト情報が生成された後、ラ

イセンス管理モジュール５１１は、受理したライセンス（トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍおよび再生期限ＡＣｐ）とチェックアウト情報とに独自の暗号化を施して暗号化機密情報を生成する（ステップＳ８９５ａ）。そして、ライセンス管理モジュール５１１は、生成した暗号化機密情報、トランザクションＩＤ、およびコンテンツＩＤを含むライセンス管理ファイルを作成してＨＤＤ５３０に記録する（ステップＳ８９６ａ）。その後、ステップＳ８９７へ移行して上述した各ステップが実行されて暗号化コンテンツデータおよびライセンスの配信動作が終了する。

【０４６３】その他の部分については、実施の形態１と同じである。実施の形態２によれば、パーソナルコンピュータに内蔵されたライセンス管理モジュールがソフトウエアによって取得した暗号化コンテンツデータのライセンスをライセンス管理デバイスによりハード的に管理されるバインディング鍵によって管理するので、ライセンス管理デバイスによって取得された暗号化コンテンツデータのライセンスと同じように「移動」という概念によって他のパーソナルコンピュータへ暗号化コンテンツデータおよびライセンスを送信することが可能である。

【０４６４】なお、実施に形態１および２において、ライセンス管理デバイス５２０には、バインディングライセンスと配信によるライセンスが格納できるとしたが、バインディングライセンス専用の管理デバイスであってもかまわない。

【０４６５】また、バインディングライセンスを指定するためにエントリ番号を指定したが専用のエントリを持ち、高いレベルのライセンスと区別して扱ってもかまわない。

【０４６６】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図１】　本発明の実施の形態１におけるデータ配信システムを概念的に説明する概略図である。

【図２】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図３】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図４】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図５】　図１に示すデータ配信システムにおける配信サーバの構成を示す概略ブロック図である。

【図６】　図１に示すデータ配信システムにおけるパーソナルコンピュータの構成を示す概略ブロック図である。

【図７】　図１に示すデータ配信システムにおける再生端末の構成を示す概略ブロック図である。

【図８】　図１に示すデータ配信システムにおけるメモリカードの構成を示す概略ブロック図である。

【図９】　図６に示すパーソナルコンピュータに内蔵されたライセンス管理デバイスの構成を示す概略ブロック図である。

【図１０】　図１に示すパーソナルコンピュータにおける機密ファイルの初期化を説明するための第１のフローチャートである。

【図１１】　図１に示すパーソナルコンピュータにおける機密ファイルの初期化を説明するための第２のフローチャートである。

【図１２】　図１に示すパーソナルコンピュータにおける機密ファイルの初期化を説明するための第３のフローチャートである。

【図１３】　図１に示すデータ配信システムにおけるセキュリティレベルの高い配信動作を説明するための第１のフローチャートである。

【図１４】　図１に示すデータ配信システムにおけるセキュリティレベルの高い配信動作を説明するための第２のフローチャートである。

【図１５】　図１に示すデータ配信システムにおけるセキュリティレベルの高い配信動作を説明するための第３のフローチャートである。

【図１６】　図１に示すデータ配信システムにおけるセキュリティレベルの高い配信動作を説明するための第４のフローチャートである。

【図１７】　図１に示すデータ配信システムにおけるセキュリティレベルの低い配信動作を説明するための第１のフローチャートである。

【図１８】　図１に示すデータ配信システムにおけるセキュリティレベルの低い配信動作を説明するための第２のフローチャートである。

【図１９】　図１に示すデータ配信システムにおけるセキュリティレベルの低い配信動作を説明するための第３のフローチャートである。

【図２０】　図１に示すデータ配信システムにおけるセキュリティレベルの低い配信動作を説明するための第４のフローチャートである。

【図２１】　図１に示すデータ配信システムにおけるセキュリティレベルの低い配信動作を説明するための第５のフローチャートである。

【図２２】　図１に示すデータ配信システムにおけるリッピングの動作を説明するための第１のフローチャートである。

【図２３】　図１に示すデータ配信システムにおけるリッピングの動作を説明するための第２のフローチャート

【図２４】　図１に示すデータ配信システムにおけるリッピングの動作を説明するための第３のフローチャートである。

【図２５】　パーソナルコンピュータのハードディスクにおけるコンテンツリストファイルの構成を示す図である。

【図２６】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動動作を説明するための第１のフローチャートである。

【図２７】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動動作を説明するための第２のフローチャートである。

【図２８】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動動作を説明するための第３のフローチャートである。

【図２９】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動動作を説明するための第４のフローチャートである。

【図３０】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックアウト動作を説明するための第１のフローチャートである。

【図３１】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックアウト動作を説明するための第２のフローチャートである。

【図３２】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックアウト動作を説明するための第３のフローチャートである。

【図３３】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックアウト動作を説明するための第４のフローチャートである。

【図３４】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックアウト動作を説明するための第５のフローチャートである。

【図３５】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックイン動作を説明するための第１のフローチャートである。

【図３６】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックイン動作を説明するための第２のフローチャートである。

【図３７】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックイン動作を説明するための第３のフローチャートである。

【図３８】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックイン動作を説明するための第４のフローチャートである。

【図３９】　再生端末における再生動作を説明するための第１のフローチャートである。

【図４０】　再生端末における再生動作を説明するための第２のフローチャートである。

【図４１】　図１に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での移動を説明するための第１のフローチャートである。

【図４２】　図１に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での移動を説明するための第２のフローチャートである。

【図４３】　図１に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での移動を説明するための第３のフローチャートである。

【図４４】　図１に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での移動を説明するための第４のフローチャートである。

【図４５】　図１に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での移動を説明するための第５のフローチャートである。

【図４６】　図１に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での移動を説明するための第６のフローチャートである。

【図４７】　図１に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での移動を説明するための第７のフローチャートである。

【図４８】　図１に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での移動を説明するための第８のフローチャートである。

【図４９】　パーソナルコンピュータのハードディスクにおけるコンテンツリストファイルの他の構成を示す図である。

【図５０】　図１に示すパーソナルコンピュータにおける機密ファイルの初期化の他の動作を説明するための第１のフローチャートである。

【図５１】　図１に示すパーソナルコンピュータにおける機密ファイルの初期化の他の動作を説明するための第２のフローチャートである。

【図５２】　図１に示すパーソナルコンピュータにおける機密ファイルの初期化の他の動作を説明するための第３のフローチャートである。

【図５３】　図１に示すデータ配信システムにおけるセキュリティレベルの低い他の配信動作を説明するための第１のフローチャートである。

【図５４】　図１に示すデータ配信システムにおけるセキュリティレベルの低い他の配信動作を説明するための第２のフローチャートである。

【図５５】　図１に示すデータ配信システムにおけるセ

キュリティレベルの低い他の配信動作を説明するための第３のフローチャートである。

【図５６】　図１に示すデータ配信システムにおけるセキュリティレベルの低い他の配信動作を説明するための第４のフローチャートである。

【図５７】　図１に示すデータ配信システムにおけるリッピングの他の動作を説明するための第１のフローチャートである。

【図５８】　図１に示すデータ配信システムにおけるリッピングの他の動作を説明するための第２のフローチャートである。

【図５９】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックアウトの他の動作を説明するための第１のフローチャートである。

【図６０】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックアウトの他の動作を説明するための第２のフローチャートである。

【図６１】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックアウトの他の動作を説明するための第３のフローチャートである。

【図６２】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックアウトの他の動作を説明するための第４のフローチャートである。

【図６３】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックアウトの他の動作を説明するための第５のフローチャートである。

【図６４】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックインの他の動作を説明するための第１のフローチャートである。

【図６５】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックインの他の動作を説明するための第２のフローチャートである。

【図６６】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックインの他の動作を説明するための第３のフローチャートである。

【図６７】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックインの他の動作を説明するための第４のフローチャートである。

【図６８】　図１に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での他の移動を説明するための第１のフローチャートである。

【図６９】　図１に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での他の移動動作を説明するための第２のフローチャートである。

【図７０】　図１に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での他の移動動作を説明するための第３のフローチャートである。

【図７１】　図１に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での他の移動動作を説明するための第４のフローチャートである。

【図７２】　図１に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での他の移動動作を説明するための第５のフローチャートである。

【図７３】　図１に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での他の移動動作を説明するための第６のフローチャートである。

【図７４】　図１に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での他の移動動作を説明するための第７のフローチャートである。

【符号の説明】

１０　配信サーバ、２０　配信キャリア、３０　インターネット網、４０　モデム、５０，８０　パーソナルコンピュータ、６０　ＣＤ、７０　ＵＳＢケーブル、９０　通信ケーブル、１００　再生端末、１１０　メモリカード、１３０ヘッドホーン、１５０　コンテンツリストファイル、１６０　暗号化機密ファイル、３０２　課金データベース、３０４　情報データベース、３０６　ＣＲＬデータベース、３０７　メニューデータベース、３０８　配信記録データベース、３１０　データ処理部、３１２，３２０，１４０４，１４０８，１４１２，１４２２，１５０４，１５１０，１５１６，５２０４，５２０８，５２１２，５２２２　復号処理部、３１３　認証鍵保持部、３１５　配信制御部、３１６，　セッションキー発生部、３１８，３２６，３２８，１４０６，１４１０，１４１７，１５０６，５２０６，５２１０，５２１７，５４０５　暗号処理部、３５０　通信装置、５１０，１１０６，１４２０，５２２０　コントローラ、５１１　ライセンス管理モジュール、５２０　ライセンス管理デバイス、５３０　ハードディスク、５４０　ＣＤ－ＲＯＭドライブ、５５０，１１１２　ＵＳＢインタフェース、５６０　キーボード、５７０　ディスプレイ、５８０，１１１４，１４２６，１５３０，５２２６　端子、１１０８　操作パネル、１１１０　表示パネル、１２００　メモリカードインタフェース、１４００，１５００，５２００　認証データ保持部、１４０２，５２０２　Ｋｍｃ保持部、１４１４，５２１４　ＫＰａ保持部、１４１５，５２１５　メモリ、１４１５Ａ，５２１５Ａ　ＣＲＬ領域、１４１５Ｂ，５２１５Ｂ　ライセン

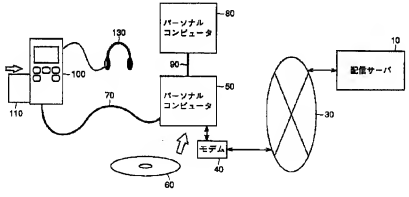
105

ス領域、１４１５Ｃ　データ領域、１４１６，５２１６　ＫＰｍｃ保持部、１４１８，５２１８　セッションキー発生部、１４２１，５２２１　Ｋｍ保持部、１４２４，５２２４　インタフェース、１４４２，１４４６

106

切換スイッチ、１５０２　Ｋｐ１保持部、１５１８　音楽再生部、１５１９　ＤＡ変換器、１５２１～１５２ｎ　ライセンス管理ファイル、１５３１～１５３ｎ　コンテンツファイル、１５５０　コンテンツ再生デバイス。

【図１】



【図２】

記号	種類	属性	特性
Dc	コンテンツデータ	コンテンツ固有	例：音楽データ、朗読データ、教材データ、画像データ Kcにて復号可能な暗号化コンテンツデータ IDc|Kcとして配信され、メモリカードに保持される
Dc-inf	付加情報	コンテンツ固有	Dcに付随する平文データ。
Kc	ライセンス	コンテンツ固有	ライセンス鍵 暗号化コンテンツデータを復号する復号鍵
ACm/ACp	ライセンス	ライセンス固有	制限情報 再生やライセンスの取り扱いに対する制限事項
トランザクションID	ライセンス	ライセンス固有	配信を特定するための管理コード
コンテンツID	ライセンス	コンテンツ固有	コンテンツを特定するための管理コード
ライセンスID	ライセンス	ライセンス固有	トランザクションID＋コンテンツIDの結称
ライセンス	ライセンス	ライセンス固有	Kc＋ACm＋ACp＋ライセンスIDの結称
CRL	禁止クラスリスト	システム共通	使用禁止鍵証データのリスト CRLの更新日(CRLdate)を含む

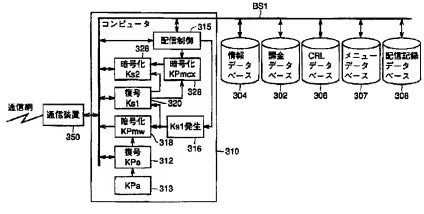
【図４】

記号	種類	特性
Kb	バインディングライセンス	バインディング鍵 ライセンスおよびチェックアウト管理情報を管理するための共通鍵
ACmb/ACpb		バインディングライセンスに対する制限情報 ACm：固定値(移動・複製禁止／再生回数制限無) ACp：固定値(ダミー／無意味)
トランザクションIDb		バインディングライセンス用のトランザクションID （ライセンスにおけるトランザクションIDとは区別可）
コンテンツIDb		バインディングID用のダミーID
バインディングID		トランザクションIDb＋コンテンツIDbの結称
チェックアウト可能数	チェックアウト管理情報	チェックアウト可能なライセンス数 チェックアウトごとに1減算し、チェックインごとに1加算する。
チェックアウト先個別ID		チェックアウト先個別公開暗号鍵KPmcx
チェックアウト時トランザクションID		チェックアウト時に用いられたトランザクションID

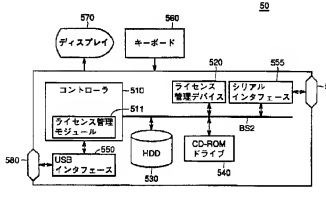
【図３】

	記号	意味	属性	特性
記憶サーバ	KPa	公開鍵証書	システム共通	認証局にて認証された認証データを提供する鍵 ※ｎリテイレベルにおけるｎ個の認証鍵KPa1(レベル1)～KPan(レベルn)がある。 メモリカードおよびコンテンツ管理モジュールと対…
	Ks1	共通鍵	セッション固有	メモリカード・ライセンス管理デバイス、ライセンス管理モジュールへのライセンス配信ごとに発生
メモリカード ライセンス管理デバイス （ハードタンパ）	KPa	公開鍵証書	システム共通	認証局にて認証された認証データを提供する鍵 配信サーバと同一
	KPmc	公開鍵号機	クラス固有	証明書Cmcとともに認証局にて暗号化された認証データとして個体nsiクラスを識別するための識別子
	Kmc	秘密復号鍵	クラス固有	公開暗号鍵KPmcにて暗号化されたデータを復号する非対称な復号鍵
ライセンス管理モジュール （ソフトタンパ）	KPmcx	公開鍵号機	個別	メモリカードごとに異なる。 xsiモジュールを識別するための識別子
	Kmcx	秘密復号鍵	個別	公開暗号鍵KPmcxにて暗号化されたデータを復号する非対称な復号鍵
	Ks2	共通鍵	セッション固有	配信サーバまたは音楽再生モジュール間のライセンスの授受ごとに発生
	Cmx	証明書	クラス証明書	メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールのクラス証明書。認証機能を有する。 (KPmx/Cmx/KPx)の形式で出荷時に記録。 ＊メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールのクラスごとに異なる。
コンテンツ再生デバイス	KPy	公開鍵号機	クラス証明	証明書Cmxとともに認証局にて暗号化された認証データとして個体yiiクラスを識別するための識別子
	Kdy	秘密復号鍵	クラス固有	公開暗号鍵KPyにて暗号化されたデータを復号する非対称な復号鍵
	Ks3	共通鍵	セッション固有	配信サーバまたは音楽再生モジュール間の再生セッションごとに発生
	Cpy	証明書	クラス証明書	コンテンツ再生デバイスのクラス証明書。認証機能を有する。 (KPpy/Cpy/KPxx)の形式で出荷時に記録。 ＊コンテンツ再生デバイスのクラスyyごとに異なる。

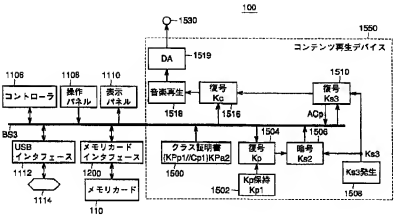
【図５】



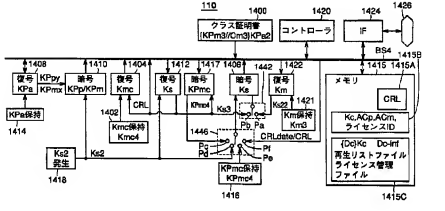
【図６】



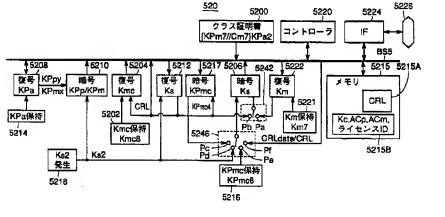
【図７】


100
1530
1550
コンテンツ再生デバイス
DA
1519
1106
1108
1110
コントローラ
操作パネル
表示パネル
音楽再生
1518
復号 Kc
1516
1510
復号 Ks3
ACp
BS3
1504
1506
USB インタフェース
メモリカード インタフェース
1112
1200
クラス証明書 [KPp1//Cp1]KPe2
1500
復号 Kp
暗号 Ke2
Ks3
Ks3発生
1114
メモリカード
110
Kp保持 Kg1
1502
1508

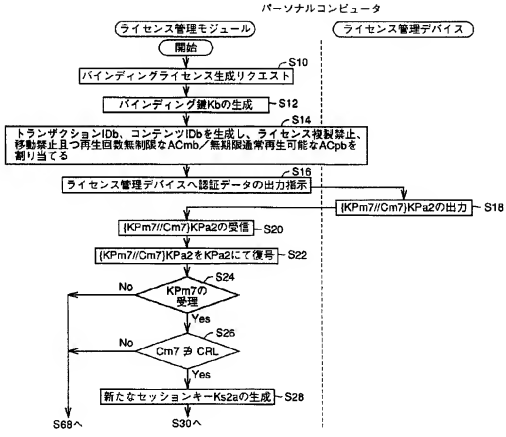
【図８】


110
1400
1420
1424
1428
クラス証明書 [KPm3//Cm3]KPe2
コントローラ
IF
BS4
1419B
1408
1410
1404
1412
1417
1406
1442
1422
1415
1415A
復号 KPs
KPpy KPmx
暗号 KPp/KPm
復号 Kmc
復号 Ks
暗号 KPmc
暗号 Ks
復号 Km
メモリ
1421
CRL
KPs保持
1414
1402
Kmc保持 Kmc4
Ks2 Ks3
Kp2 Cp
Pb, Pa
Km保持 Km3
Ks2保持
CRLdate/CRL
1446
Pg
Rd
Pf
Pe
Kc,ACp,ACm, ライセンスID
(De)Kc De-inf
再生リストファイル ライセンス管理 ファイル
Ks2 発生
Ks2
KPmc保持 KPmc4
1418
1416
1415C

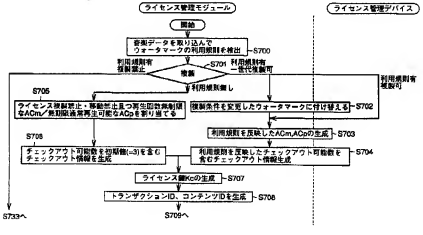
【図９】


520
5200
5220
5224
5225
クラス証明書 [KPm7//Cm7]KPe2
コントローラ
IF
BS5
5208
5210
5204
5212
5217
5206
5242
5222
5215
5215A
復号 KPs
KPpy KPmx
暗号 KPp/KPm
復号 Kmc
復号 Ks
暗号 KPmc
暗号 Ks
復号 Km
メモリ
5221
CRL
KPmc4
KPs保持
5214
5202
Kmc保持 Kmc8
5246
Km保持 Km7
Kc,ACp,ACm, ライセンスID
Kp2 Cp
Pb, Pa
CRLdate/CRL
Pg
Rd
Pf
Pe
5215B
Ks2 発生
Ks2
KPmc保持 KPmc6
5218
5216

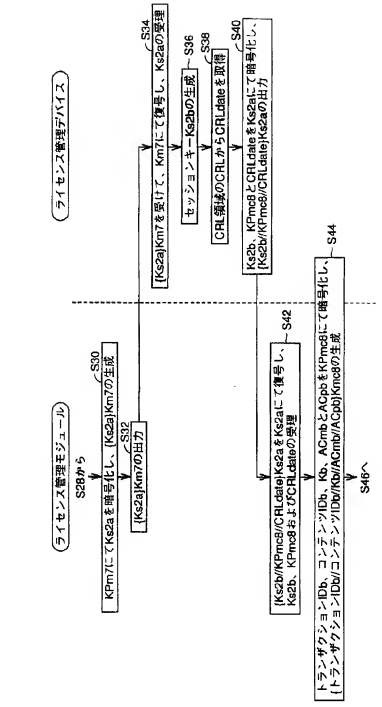
【図１０】


パーソナルコンピュータ
ライセンス管理モジュール
ライセンス管理デバイス
開始
S10
バインディングライセンス生成リクエスト
S12
バインディング鍵Kbの生成
S14
トランザクションIDb、コンテンツIDbを生成し、ライセンス複製禁止、移動禁止且つ再生回数無制限なACmb／無期限通常再生可能なACpbを割り当てる
S16
ライセンス管理デバイスへ認証データの出力指示
{KPm7//Cm7}KPa2の出力
S18
{KPm7//Cm7}KPa2の受信
S20
{KPm7//Cm7}KPa2をKPa2にて復号
S22
S24
KPm7の受理
No
Yes
S25
Cm7 為 CRL
No
Yes
新たなセッションキーKs2aの生成
S28
S68へ
S30へ

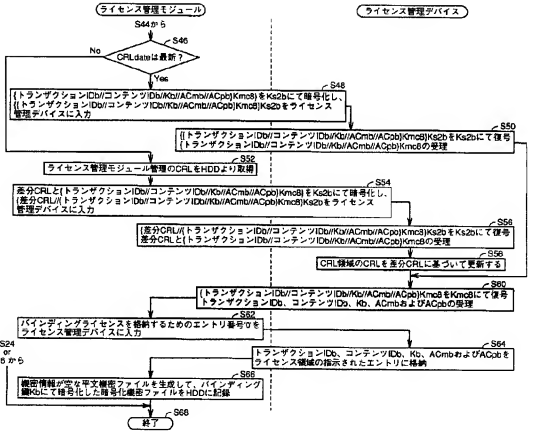
【図２２】


ライセンス管理モジュール
ライセンス管理デバイス
開始
S700
S701
S702
S703
S704
S705
S706
S707
S708
S733へ
S709へ

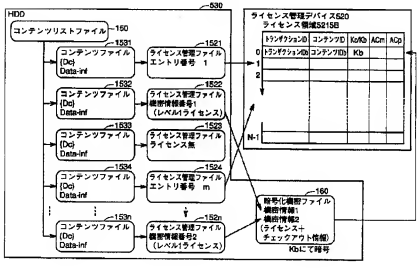
【図１１】


ライセンス管理モジュール
ライセンス管理デバイス
S28から
KPm7にて Ks2a を暗号化し、[Ks2a]Km7の生成
S30
[Ks2a]Km7の出力
S32
[Ks2a]Km7を受けて、Km7にて復号し、Ks2aの受理
S34
セッションキー Ks2bの生成
S36
CRL領域のCRLからCRL.dateを取得
S38
Ks2b、KPmc8とCRL.dateをKs2aにて暗号化し、
[Ks2b/KPmc8/CRL.date]Ks2a
S40
[Ks2b/KPmc8/CRL.date]Ks2a を Ks2a にて復号し、
Ks2b、KPmc8 および CRL.date の受理
S42
[Ks2b/KPmc8/CRL.date]Ks2a
[Ks2b/KPmc8/CRL.date]Ks2aの出力
トランザクションIDb、コンテンツIDb、Kb、ACmbとACpbをKPmc8にて暗号化し、
[トランザクションID/コンテンツID/Kb/ACmb/ACpb]Kmc8の生成
S44
S46へ

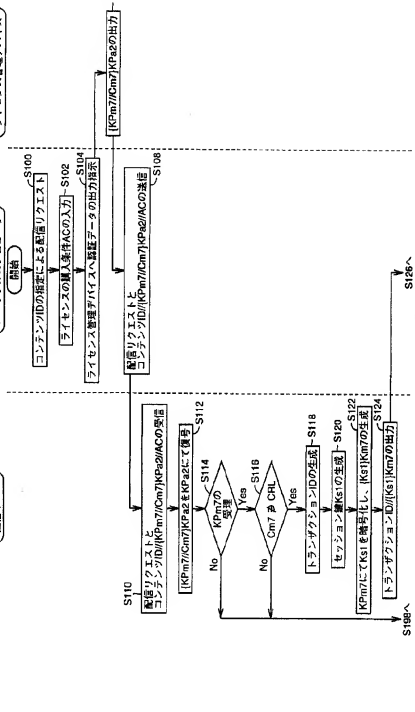
【図１２】


ライセンス管理モジュール
ライセンス管理デバイス
S44から
S45
No
CRLdateは最新？
Yes
S48
{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8)をKs2bにて暗号化し、
{{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8}Ks2bをライセンス管理デバイスに入力
S50
{{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8}Ks2bをKs2bにて復号
{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8の受理
S52
ライセンス管理モジュール管理のCRLをHDDより取得
S54
差分CRLと{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8}をKs2bにて暗号化し、
{差分CRL//{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8}Ks2bをライセンス管理デバイスに入力
S56
{差分CRL//{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8}Ks2bをKs2bにて復号
差分CRLと{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8の受理
S58
CRL領域のCRLを差分CRLに基づいて更新する
S60
{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8をKmc8にて復号
トランザクションIDb、コンテンツIDb、Kb、ACmbおよびACpbの受理
S62
バインディングライセンスを格納するためのエントリ番号Oを
ライセンス管理デバイスに入力
S24
or
S25から
S64
トランザクションIDb、コンテンツIDb、Kb、ACmbおよびACpbを
ライセンス領域の指示されたエントリに格納
S66
機密情報が空な平文機密ファイルを生成して、バインディング鍵Kbにて暗号化した暗号化機密ファイルをHDDに記録
S68
終了

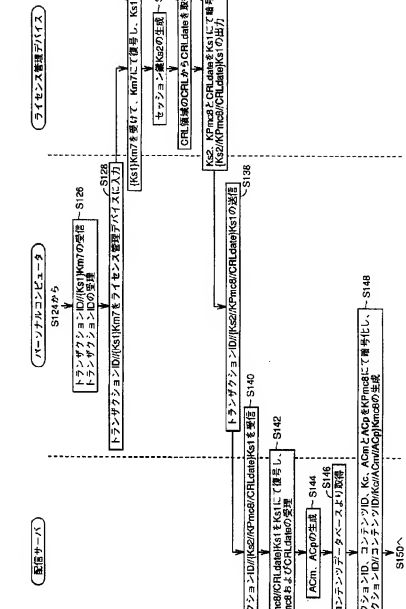
【図２５】


HDD
530
コンテンツリストファイル
160
1531
コンテンツファイル
{Dc}
Data-inf
1521
ライセンス管理ファイル
エントリ番号　1
1532
コンテンツファイル
{Dc}
Data-inf
1522
ライセンス管理ファイル
機密情報番号1
（レベル1ライセンス）
1533
コンテンツファイル
{Dc}
Data-inf
1523
ライセンス管理ファイル
ライセンス無
1534
コンテンツファイル
{Dc}
Data-inf
1524
ライセンス管理ファイル
エントリ番号　m
153n
コンテンツファイル
{Dc}
Data-inf
152n
ライセンス管理ファイル
機密情報番号2
（レベル1ライセンス）
ライセンス管理デバイス520
ライセンス管理部518
トランザクションID
コンテンツID
KcKb
ACm
Kcp
0
トランザクションIDb
コンテンツIDb
Kb
1
2
N-1
160
暗号化機密ファイル
機密情報1
機密情報2
（ライセンス＋
チェックアウト情報）
Kbにて暗号

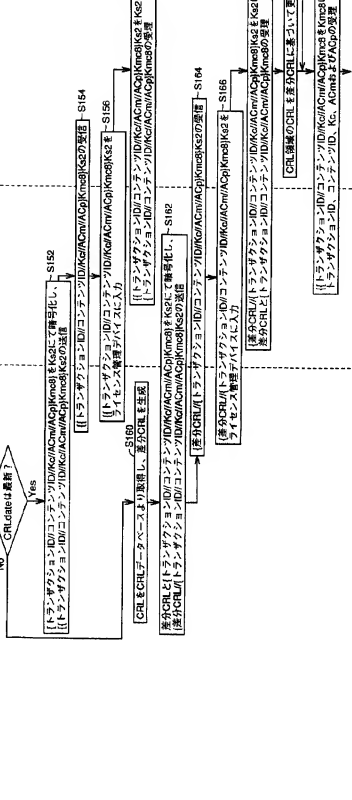
【図１３】


配信サーバ
パーソナルコンピュータ
ライセンス管理デバイス
開始
S100
コンテンツIDの指定による配信リクエスト
S102
ライセンスの購入条件ACの入力
S104
ライセンス管理デバイスへ録音データの出力指示
S106
[KPm7/iCm7]KPa2の出力
S108
配信リクエストと
コンテンツID//[KPm7/iCm7]KPa2//ACの送信
S110
配信リクエストと
コンテンツID//[KPm7/iCm7]KPa2//ACの受信
[KPm7/iCm7]KPa2をKPa2に一て保存
S112
S114
KPm7の
整理
No
Yes
S116
Cm7 ≠ CRL
No
Yes
トランザクションIDの生成
S118
セッション鍵Ks1の生成
S120
KPmのにてKs1を暗号化し、[Ks1]Km7の生成
S122
トランザクションID//[Ks1]Km7の出力
S124
S126へ
S128へ

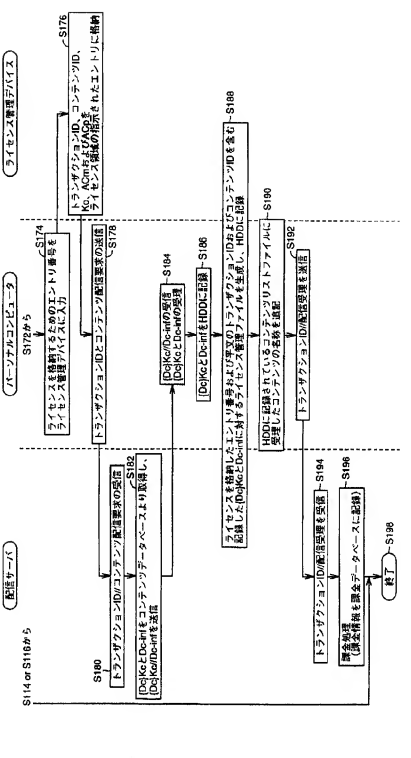
【図１４】


配信サーバ
パーソナルコンピュータ
ライセンス管理デバイス
S124から
トランザクションID//Ks1//Kmの受信
S126
トランザクションID//Ks1//Kmを受けて、Kmにて復号し、Ks1の取得
S130
トランザクションID//Ks1//Kmをライセンス管理デバイスに入力
S128
セッションKs2の生成
S132
S134
CRL領域のCRLデータ取得
S136
Ks2、KPmcdとCRLdate#Ks1にて暗号化し、
(Ks2//KPmcd//CRLdate#Ks1)の出力
トランザクションID//(Ks2//KPmcd//CRLdate#Ks1)の送信
S138
トランザクションID//Ks2//KPmcd//CRLdate#Ks1を受信
S140
(Ks2//KPmcd//CRLdate#Ks1をKs1にて復号し、
Ks2、KPmcdおよびCRLdate#の受理
S142
ACm、ACpの生成
S144
S146
Ksをコンテンツデータベースより取得
トランザクションID、Ks、ACm上ACpをKPmcdにて暗号化し、
トランザクションID//(Ks//ACm//ACp)//mcdの生成
S148
S150へ

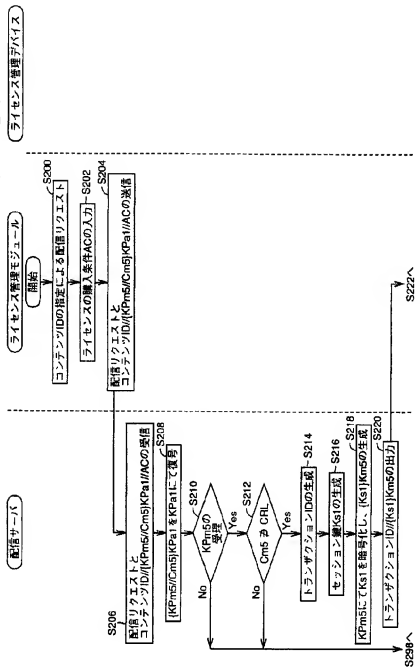
【図１５】


配信サーバ
パーソナルコンピュータ
ライセンス管理デバイス
S148
n*5
S150
CRLdate≠最新？
No
Yes
{{トランザクションID//コンテンツID/Kci/ACm/ACpk(Kmcd)をKs2にて暗号化し、
{{トランザクションID//コンテンツID/Kci/ACm/ACpk(Kmcd)Ks2の送信
S152
{{トランザクションID//コンテンツID/Kci/ACm/ACpk(Kmcd)Ks2の受信
S154
{{トランザクションID//コンテンツID/Kci/ACm/ACpk(Kmcd)Ks2 を
ライセンス管理デバイスに入力
S156
CRL をCRLデータベースより取得し、差分CRL を生成
S160
{{トランザクションID//コンテンツID/Kci/ACm/ACpk(Kmcd)Ks2 をKs2にて復号
{{トランザクションID//コンテンツID/Kci/ACm/ACpkKmcdの受信
差分CRL={{トランザクションID//コンテンツID/Kci/ACm/ACpk(Kmcd)Ks2}Ks2
差分CRL={{トランザクションID//コンテンツID/Kci/ACm/ACpk(Kmcd)Ks2}Ks2
{{差分CRL}={トランザクションID//コンテンツID/Kci/ACm/ACpk(Kmcd)Ks2}Ks2
S162
{{差分CRL}={トランザクションID//コンテンツID/Kci/ACm/ACpk(Kmcd)Ks2}Ks2の送信
S164
{{差分CRL}={トランザクションID//コンテンツID/Kci/ACm/ACpk(Kmcd)Ks2}Ks2の受信
S166
{{差分CRL}={トランザクションID//コンテンツID/Kci/ACm/ACpk(Kmcd)Ks2 を
ライセンス管理デバイスに入力
S168
{差分CRL}={トランザクションID//コンテンツID/Kci/ACm/ACpk(Kmcd)Ks2 をKs2にて復号
差分CRLと{トランザクションID//コンテンツID/Kci/ACm/ACpkKmcdの受理
S170
CRL保管庫のCRL を差分CRL に基づいて更新する
S172
{{トランザクションID//コンテンツID/Kci/ACm/ACpkKmcdをKmcdにて復号
トランザクションID、コンテンツID、Kci、ACmおよびACpkの受理
S174へ

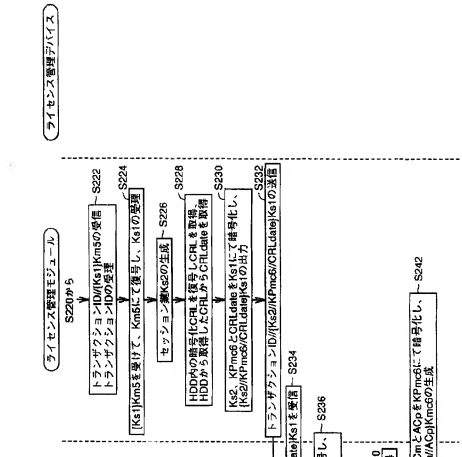
【図１６】


配信サーバ
パーソナルコンピュータ
ライセンス管理デバイス
S114 or S116から
S180
トランザクションID//コンテンツ配信要求の送信
S182
[Dc]Kc,[Dc-inf]をコンテンツデータベースより取得し、
[Dc]Kc//[Dc-inf]を送信
S172から
ライセンスを格納するためのエントリ番号を
ライセンス管理デバイスに入力
S174
トランザクションID,コンテンツID,
Kc, Kcm,およびACLを
ライセンス格納の指示されたエントリに格納
S176
トランザクションIDとコンテンツ配信要求の送信
S178
[Dc]Kc//Dc-infの受信
[Dc]Kcと[Dc-inf]をHDDに記録
S184
S186
ライセンスを格納したエントリ番号およびトランザクションIDおよびコンテンツIDを含む
記録した[Dc]Kc,[Dc-inf]に対するライセンス管理ファイルを生成し、HDDに記録
S188
HDDに記録されているコンテンツリストファイルに
登録したコンテンツの追加を記録
S190
トランザクションIDの配信要求を送信
S192
トランザクションIDの配信受理を受信
S194
課金処理
（課金情報を課金データベースに記録）
S196
終了
S198

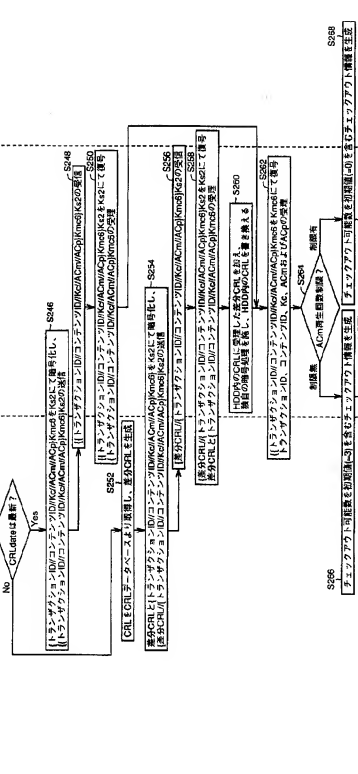
【図１７】


パーソナルコンピュータ
配信サーバ
ライセンス管理モジュール
ライセンス管理デバイス
開始
S200
コンテンツIDの指定による配信リクエスト
S202
ライセンスの購入条件ACの入力
S204
配信リクエストと
コンテンツID//(KPms5/Cms5)KPa11/ACの送信
S206
配信リクエストと
コンテンツID//(KPms5/Cms5)KPa11/ACの受信
S208
(KPms5//Cms5)KPa1をKPa1cにて復号
S210
KPms5の
受理
No
Yes
S212
Cms5 ≠ CRL
No
Yes
トランザクションIDの生成
S214
セッション鍵Ks1の生成
S216
KPms5にてKs1を暗号化し、(Ks1)Kms5の生成
S218
トランザクションID//(Ks1)Kms5の出力
S220
S222へ
S238へ

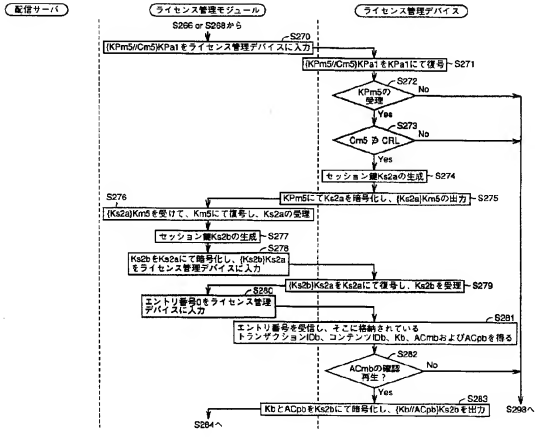
【図１８】


配信サーバ
ライセンス管理モジュール
ライセンス管理デバイス
S220から
トランザクション/ID//Ks1|Kms5の受信
トランザクション/IDの処理
S222
S224
[Ks1]Kms5を受けて、Kms5にて復号し、Ks1の処理
セッション鍵Ks2の生成
S226
S228
HDD内の暗号化CRLを復号しCRLを取得
HDDから取得したCRLからCRLdateを取得
S230
Ks2、KPmc6とCRLdateをKs1にて暗号化し、
[Ks2/KPmc6/CRLdate]Ks1の出力
S232
トランザクション/ID//[Ks2/KPmc6/CRLdate]Ks1の送信
トランザクション/ID//Ks2/KPmc6/CRLdate|Ks1を受信
S234
[Ks2/KPmc6/CRLdate]Ks1をKs1にて復号し、
Ks2、KPmc6およびCRLdateの処理
S236
ACm、ACpの生成
S238
S240
Kcをコンテンツデータベースより取得
トランザクション/ID、コンテンツID、Kc、ACmとACpをKPmc6にて暗号化し、
[トランザクション/ID//コンテンツID//Kc//ACm//ACp]Kmc6の生成
S242
S244へ

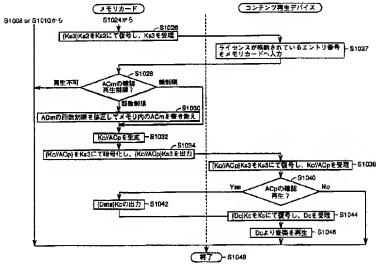
【図１９】


配信サーバ
ライセンス管理モジュール
ライセンス管理デバイス
S242#5
CRLdateは最新？
No
Yes
S244
S246
S248
S250
S252
S254
S256
S258
S260
S262
S264
S266
S268
CRLとCRLデータベースより取得し、差分CRLを生成
差分CRLを{トランザクションID/コンテンツID/Kd/ACm/ACp}Kmdsにて暗号化し、
{トランザクションID/コンテンツID/Kd/ACm/ACp}Kd209送信
差分CRL/{トランザクションID/コンテンツID/Kd/ACm/ACp}Kmds/Kd209受信
差分CRL/{トランザクションID/コンテンツID/Kd/ACm/ACp}Kmds/Kd2にて復号
差分CRLを{トランザクションID/コンテンツID/Kd/ACm/ACp}Kmds/Kd209受信
HDDPK内CRLに保持した差分CRLを取り出し、
署名の検証を行い、HDDPK内CRLを書き換える
{トランザクションID/コンテンツID/Kd/ACm/ACp}Kmdsを{トランザクションID/コンテンツID/Kd/ACm/ACp}Kmdsにて復号
{トランザクションID/コンテンツID/Kd/ACm/ACp}Kmdsを{トランザクションID/コンテンツID/Kd/ACm/ACp}Kd2にて復号
ACm再生回数制限？
制限無
制限有
チェックアウト可能数を初期値(=0)をもとにチェックアウト情報を生成
チェックアウト可能数を初期値(=n)から1減算
チェックアウト情報を生成
S270へ

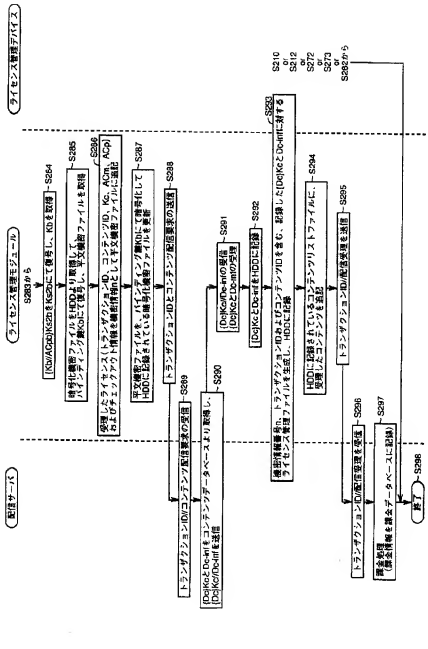
【図２０】


配信サーバ
ライセンス管理モジュール
ライセンス管理デバイス
S266 or S298から
S270
[KPm5/Cm5]KPa1をライセンス管理デバイスに入力
[KPm5/Cm5]KPa1をKPa1にて復号
S271
S272
KPmbの受理
No
Yes
S273
Cm5 ≠ CRL
No
Yes
セッション鍵Ks2aの生成
S274
S276
[Ks2a]Km5を受けて、Km5にて復号し、Ks2aの受理
KPm5にてKs2aを暗号化し、[Ks2a]Km5の出力
S275
セッション鍵Ks2bの生成
S277
S278
Ks2bをKs2aにて暗号化し、[Ks2b]Ks2aをライセンス管理デバイスに入力
[Ks2b]Ks2aをKs2aにて復号し、Ks2bを受理
S279
S280
エントリ番号0をライセンス管理デバイスに入力
S281
エントリ番号を受信し、そこに格納されているトランザクションIDb、コンテンツIDb、Kb、ACmbおよびACpbを得る
S282
ACmbの確認
再生？
No
Yes
S283
KbとACpbをKs2bにて暗号化し、{Kb//ACpb}Ks2bを出力
S298へ
S284へ

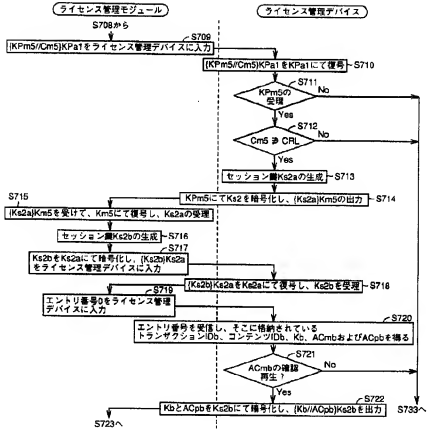
【図４０】


メモリカード
コンテンツ再生デバイス
S1024から
S1026
[Ks3]Ks2をKs2にて復号し、Ks3を受理
ライセンスが格納されているエントリ番号をメモリカードへ入力
S1027
S1028
ACmの確認
再生/録画
再生:不可
録画:制限
S1030
ACmの回数制御を施したメモリ内のACmを書き換え
Kc//ACpを生成
S1032
S1034
[Kc//ACp]をKs3にて暗号化し、{Kc//ACp}Ks3を出力
[Kc//ACp]Ks3をKs3にて復号し、Kc//ACpを受理
S1036
S1040
ACpの確認
再生？
Yes
No
[Data]Kcの出力
S1042
[Dc]Kcを Kcにて復号し、Dcを受理
S1044
Dcより複製を再生
S1046
終了
S1048
S1008 or S1010から

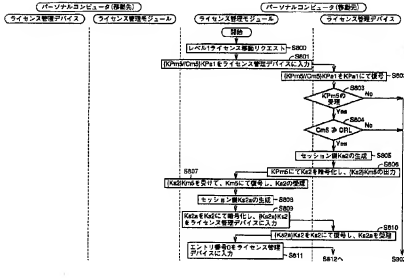
【図２１】


配信サーバ
ライセンス管理モジュール
ライセンス管理デバイス
S263から
{Ku'AOdpqNKdn}をKdpNoにて復号し、Kdを取得
S264
{Ku'AOdpqNKdn}をKdpNoにて復号し、Kdを取得
S264
特定情報ファイルおよびIDを用いて、ライセンス情報ファイルを取得
S265
特定情報ファイルおよびIDを用いて、ライセンス情報ファイルを取得
S265
S266
受理したライセンス{トランザクションID、コンテンツID、No、ACm、ACp}とICチェックアウト情報を最終情報として更新情報ファイルに追記
S267
特定情報ファイルを、バインディング情報HDDに対応付けて{トランザクションID、コンテンツID}と{配信要求}の送信
S268
トランザクションIDとコンテンツ配信要求の送信
S269
{DcsKc'とDc-inf'をライセンス管理モジュールへ}
{DcsKc'とDc-inf'を送信
検索情報等から、トランザクションIDおよびコンテンツIDを得る。取得した{EKdcKc'とDc-inf'}を{DcsKc'とDc-inf'}を含むライセンス管理ファイルを生成し、HDDに記録
S270
S271
S272
S273
S274
S275
S276
S277
S278
S279
S280
S281
S282
S283
S284
S285
S286
S287
S288
S289
S290
S291
S292
S293
S294
S295
S296
S297
S298
{DcsKc'とDc-inf'}を受信
{DcsKc'とDc-inf'}を受信
{DcsKc'とDc-inf'}の要求
{DcsKc'とDc-inf'}の要求
{DcsKc'とDc-inf'}をHDDに記録
{DcsKc'とDc-inf'}をHDDに記録
{EKdcKc'とDc-inf'}を含む、記録した{EKdcKc'とDc-inf'}に対する
{EKdcKc'とDc-inf'}に対する
HDDに記録されているライセンス管理ファイルに、{EKdcKc'とDc-inf'}を含むライセンス管理ファイルを記録
トランザクションIDの配信処理を通知
トランザクションIDの配信管理要求を受理
再生処理
{復号情報}を読みデータベースに記録
終了
S299から
S285から

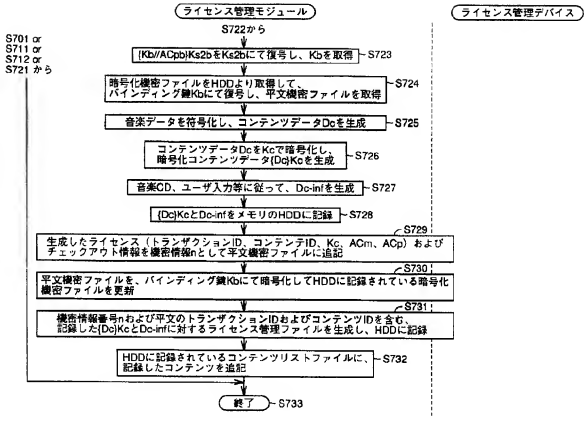
【図２３】


ライセンス管理モジュール
ライセンス管理デバイス
S708から
S709
[KPm5/Cm5]KPa1をライセンス管理デバイスに入力
[KPm5/Cm5]KPa1をKPa1にて復号
S710
S711
KPm5の受理
No
Yes
S712
Cm5 ∋ CRL
No
Yes
セッション鍵Ks2aの生成
S713
S715
KPm5にてKs2を暗号化し、(Ks2a)Km5の出力
S714
[Ks2a]Km5を受けて、Km5にて復号し、Ks2aの受理
セッション鍵Ks2bの生成
S716
S717
Ks2bをKs2aにて暗号化し、[Ks2b]Ks2aをライセンス管理デバイスに入力
[Ks2b]Ks2aをKs2aにて復号し、Ks2bを受理
S718
S719
エントリ番号0をライセンス管理デバイスに入力
S720
エントリ番号を受理し、そこに格納されているトランザクションDb、コンテンツIDb、Kb、ACmbおよびACpbを得る
S721
ACmbの確認再生？
No
Yes
S722
KbとACpbをKs2bにて暗号化し、(Kb//ACpb)Ks2bを出力
S733へ
S723へ

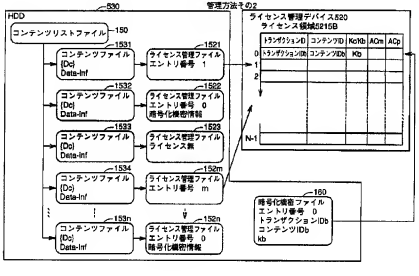
【図４１】


パーソナルコンピュータ(携帯先)
ライセンス管理デバイス
ライセンス管理モジュール
パーソナルコンピュータ(携帯前)
ライセンス管理モジュール
ライセンス管理デバイス
開始
レベル1ライセンス移動リクエスト
S801
[KPm5/Cm5]KPa1をライセンス管理デバイスに入力
S802
[KPm5/Cm5]KPa1をKPa1にて復号
S803
KPm5の受理
No
Yes
S804
Cm5 ∋ CRL
No
Yes
セッション鍵Ks2の生成
S805
S806
KPm5にてKs2を暗号化し、Ks2Km5の出力
S807
[Ks2]Km5を受けて、Km5にて復号し、Ks2の受理
セッション鍵Ks3aの生成
S808
S809
Ks3aをKs2にて暗号化し、[Ks3a]Ks2をライセンス管理デバイスに入力
S810
[Ks3a]Ks2をKs2にて復号し、Ks3aを受理
エントリ番号0をライセンス管理デバイスに入力
S811
S812へ
S803へ

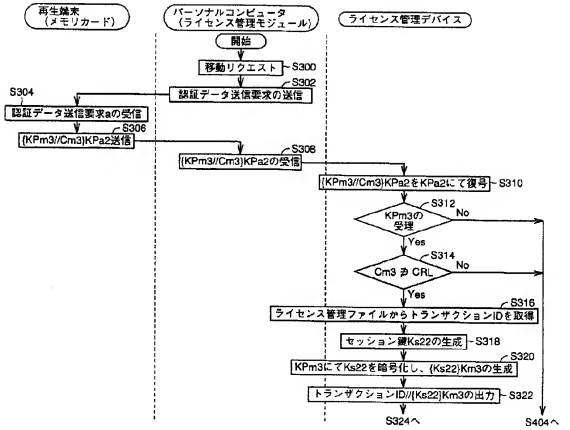
【図２４】


ライセンス管理モジュール
ライセンス管理デバイス
S722から
S701 or
S711 or
S712 or
S721 から
[Kb//ACpb]Ks2bをKs2bにて復号し、Kbを取得
S723
暗号化機密ファイルをHDDより取得して、
バインディング鍵Kbにて復号し、平文機密ファイルを取得
S724
音楽データを符号化し、コンテンツデータDcを生成
S725
コンテンツデータDcをKcで暗号化し、
暗号化コンテンツデータ[Dc]Kcを生成
S726
音楽CD、ユーザ入力等に従って、Dc-infを生成
S727
{Dc}KcとDc-infをメモリのHDDに記録
S728
S729
生成したライセンス（トランザクションID、コンテンツID、Kc、ACm、ACp）およびチェックアウト情報を機密情報nとして平文機密ファイルに追記
S730
平文機密ファイルを、バインディング鍵Kbにて暗号化してHDDに記録されている暗号化機密ファイルを更新
S731
機密情報番号nおよび平文のトランザクションIDおよびコンテンツIDを含む、記録した{Dc}KcとDc-infに対するライセンス管理ファイルを生成し、HDDに記録
HDDに記録されているコンテンツリストファイルに、記録したコンテンツを追記
S732
終了
S733

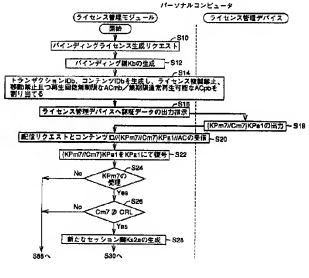
【図４９】


HDD
530
管理方法その2
コンテンツリストファイル
150
1531
コンテンツファイル
{Dc}
Data-Inf
1521
ライセンス管理ファイル
エントリ番号　1
1532
コンテンツファイル
{Dc}
Data-Inf
1522
ライセンス管理ファイル
エントリ番号　0
暗号化機密情報
1533
コンテンツファイル
{Dc}
Data-Inf
1523
ライセンス管理ファイル
ライセンス無
1534
コンテンツファイル
{Dc}
Data-Inf
152m
ライセンス管理ファイル
エントリ番号　m
153n
コンテンツファイル
{Dc}
Data-Inf
152n
ライセンス管理ファイル
エントリ番号　0
暗号化機密情報
ライセンス管理デバイス520
ライセンス領域5215B
トランザクションID
コンテンツID
Kc/Kb
ACm
ACp
0
1
2
N-1
トランザクションIDb
コンテンツIDb
Kb
160
暗号化機密ファイル
エントリ番号　0
トランザクションIDb
コンテンツIDb
Kb

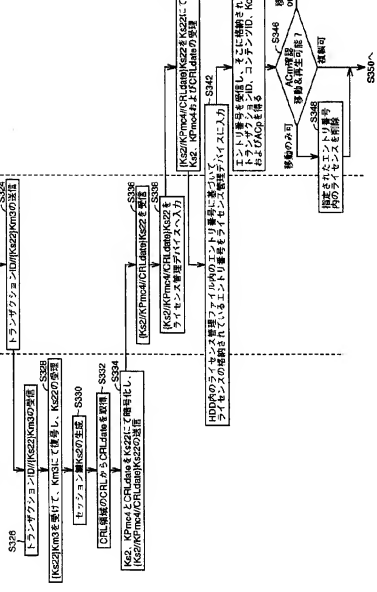
【図２６】


再生端末
（メモリカード）
パーソナルコンピュータ
（ライセンス管理モジュール）
ライセンス管理デバイス
開始
移動リクエスト
S300
S302
認証データ送信要求の送信
S304
認証データ送信要求aの受信
S306
{KPm3//Cm3}KPa2送信
S308
{KPm3//Cm3}KPa2の受信
{KPm3//Cm3}KPa2をKPa2にて復号
S310
S312
KPm3の受理
No
Yes
S314
Cm3 ≠ CRL
No
Yes
S316
ライセンス管理ファイルからトランザクションIDを取得
セッション鍵Ks22の生成
S318
S320
KPm3にてKs22を暗号化し、{Ks22}Km3の生成
トランザクションID,/{Ks22}Km3の出力
S322
S324へ
S404へ

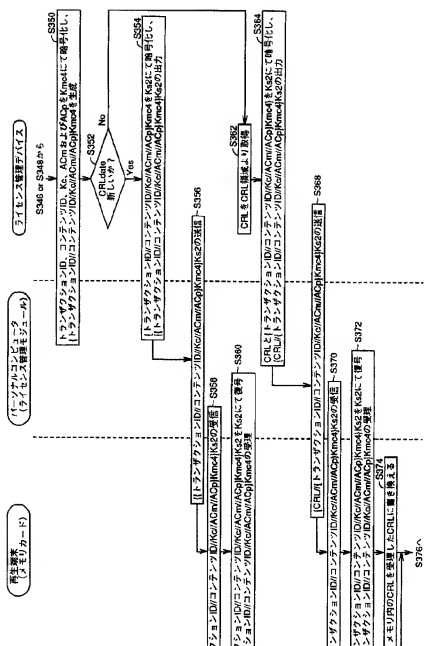
【図５０】


パーソナルコンピュータ
ライセンス管理モジュール
ライセンス管理デバイス
開始
S10
バインディングライセンス生成リクエスト
バインディング鍵Kbの生成
S12
S14
S16
ライセンス管理デバイスへ認証データの出力許可
S18
{KPm7//Cm7}KPa1の出力
S20
{KPm7//Cm7}KPa1をKPa1にて復号
S22
S24
No
Yes
S25
No
Yes
S26
S86へ
S30へ

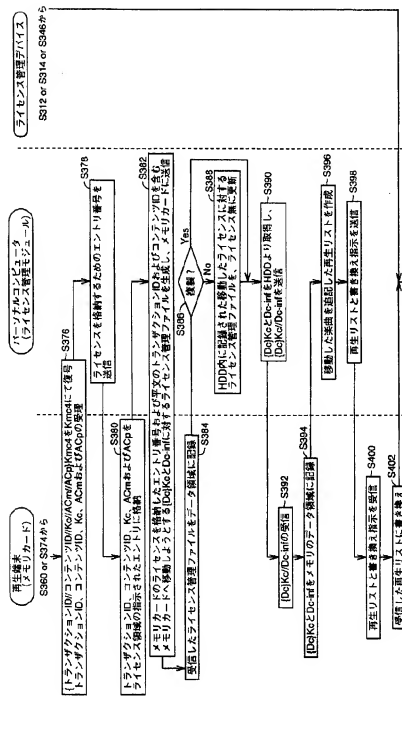
【図２７】


再生装置
（メモリカード）
（インテグラルコンピュータ
（ライセンス管理モジュール））
ライセンス管理デバイス
S322から
S324
トランザクション-ID//[Ks22]Km3の送信
S326
トランザクション-ID//[Ks22]Km3の受信
S328
[Ks22]Km3を受け取って、Km3にて復号し、Ks22の受理
S330
セッション鍵Ks20の生成
S332
CRL情報のCRLバージョンとCRLdateを取得
S334
Ks2、KPmc4とCRLdateをKs22にて暗号化し、
[Ks20/KPmc4/CRLdate]Ks22の送信
S336
[Ks2/KPmc4/CRLdate]Ks22を受信
S338
[Ks20/KPmc4/CRLdate]Ks22を
ライセンス管理デバイスへ入力
S340
[Ks22/KPmc4/CRLdate]Ks22をKs22にて復号し、
Ks2、KPmc4およびCRLdateの受理
HDD内のライセンス管理ファイル内のエントリ番号に基づいて、
ライセンスの格納されているエントリ番号をライセンス管理デバイスに入力
S342
S344
エントリ番号を受信し、それに格納されている
トランザクションID、コンテンツID、Kc、ACm
およびMACpを得る
移動のみ可
S346
ACmの内容が
移動許可か？
移動/複製禁止
or 再生不可
S348
指定されたエントリ番号
内のライセンスを削除
複製可
S350へ
S404へ

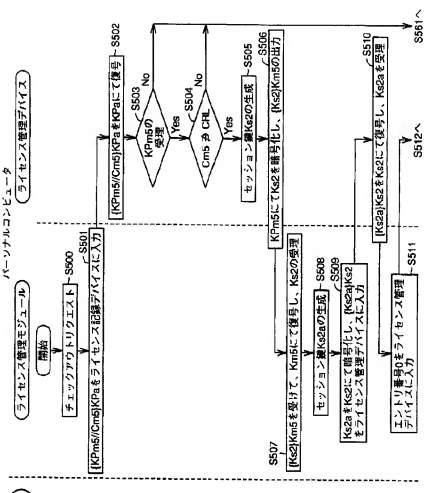
【図２８】


再生要求
（メモリカード）
「ノンアルコンテンツ
（ライセンス管理モジュール）」
ライセンス管理デバイス
S346 or S348から
S350
S352
No
Yes
S354
S356
S358
S360
S362
S364
S368
S370
S372
S374
S376へ

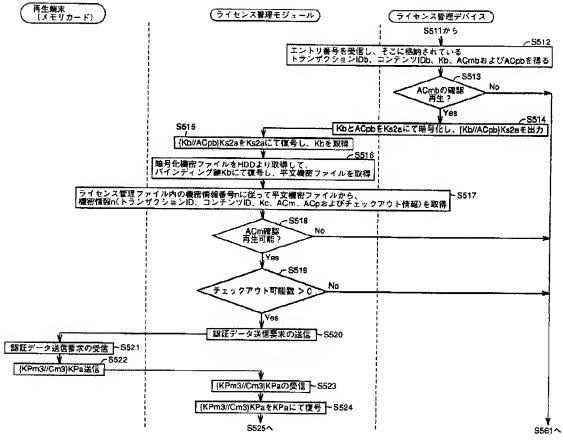
【図２９】


再生機
(メモリカード)
S380 or S374から
ユーザコマンドデータ
(ライセンス管理モジュール)
ライセンス管理デバイス
S312 or S314 or S346から
トランザクション開始
トランザクションID/コンテンツID/Kci/ACmi/ACpi/Kmcrtにて復号
トランザクションID、コンテンツID、Kc、ACmiおよびACpiの受理
S376
ライセンスを格納するためのエントリ番号を送信
S378
トランザクションID、コンテンツID、Kc、ACmiおよびACpiを送信
S380
ライセンス領域の指示されたエントリに格納
S382
メモリカードのライセンス領域にあるエントリ番号およびパスワードのトランザクション開始
メモリカードの移動によるDcli/Kci/Dcliに対するライセンス管理ファイルを生成、メモリカードに送信
S384
受信したライセンス管理ファイルをデータ領域に記録
S386
残数？
Yes
No
S388
HDD内に記録されたDcli/Kci/Dcliに対するライセンス管理ファイルを、ライセンス数に更新
Dcli/Kci/Dcliの受信
S392
Dcli/Kci/Dcliの送信
S390
Dcli/Kci/Dcliをメモリのデータ領域に記録
S394
Dcli/Kci/Dcliをkey1/key2より復号し、
Dcli/Kci/Dcliを送信
移動した楽曲を追加した再生リストを作成
S396
再生リストと書き換え指示を送信
S398
再生リストと書き換え指示を受信
S400
受信した再生リストに書き換え
S402
終了
S404

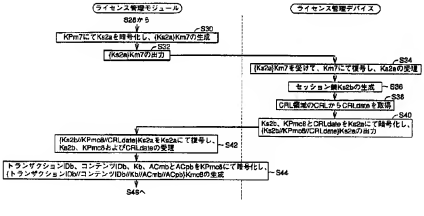
【図３０】


パーソナルコンピュータ
ライセンス管理モジュール
ライセンス管理デバイス
再生端末
(メモリカード)
開始
チェックアウトリクエスト
S500
S501
[KPm5/Cm5]KPaをライセンス記録デバイスに入力
[KPm5/Cm5]KPaをKPa1にて復号
S502
KPm5の受理
S503
No
Yes
Cm5 = Cm6
S504
No
Yes
セッション鍵Ks2の生成
S505
S506
KPm5にてKs2を暗号化し、[Ks2]Km5の出力
S507
[Ks2]Km5を受けて、Km5にて復号し、Ks2の受理
セッション鍵Ks2aの生成
S508
S509
Ks2aをKs2にて暗号化し、[Ks2a]Ks2をライセンス管理デバイスに入力
[Ks2a]Ks2をKs2にて復号し、Ks2aを受理
S510
エントリ番号のライセンス管理デバイスに入力
S511
S512
S551

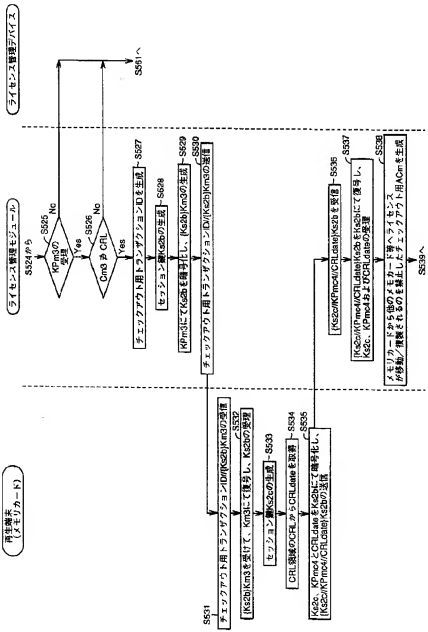
【図３１】


再生端末
（メモリカード）
ライセンス管理モジュール
ライセンス管理デバイス
S511から
S512
エントリ番号を受信し、そこに格納されている
トランザクションID、コンテンツID、Kb、ACmbおよびACpbを得る
S513
ACmbの確認
再生？
No
Yes
S514
KbとACpbをKs2eにて暗号化し、[Kb//ACpb]Ks2eを出力
S515
[Kb//ACpb]Ks2aをKs2aにて復号し、Kbを取得
S516
暗号化機密ファイルをHDDより取得して、
バインディング鍵Kbにて復号し、平文機密ファイルを取得
S517
ライセンス管理ファイル内の機密情報番号nに従って平文機密ファイルから、
機密情報n(トランザクションID、コンテンツID、Kc、ACm、ACpおよびチェックアウト情報)を取得
S518
ACm確認
再生可能？
No
Yes
S519
チェックアウト可能数＞0
No
Yes
S520
認証データ送信要求の送信
S521
認証データ受信
S522
[KPm3//Cm3]KPa送信
S523
[KPm3//Cm3]KPaの受信
S524
[KPm3//Cm3]KPaをKPaにて復号
S525へ
S561へ

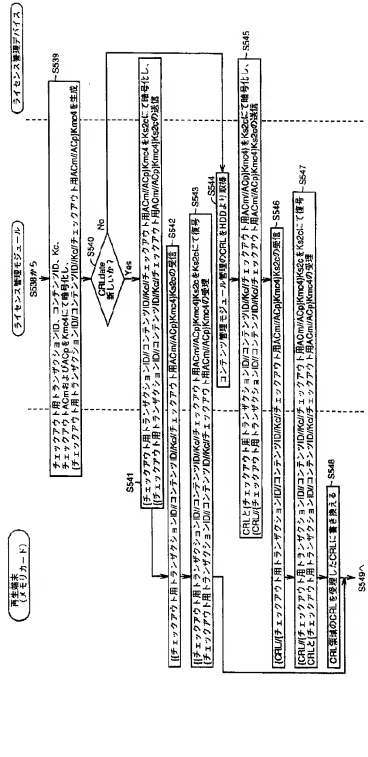
【図５１】


ライセンス管理モジュール
ライセンス管理デバイス
S28から
S30
KPm7にてKs2aを暗号化し、[Ks2a]Km7の生成
S32
[Ks2a]Km7の出力
S34
[Ks2a]Km7を受け取り、Km7にて復号し、Ks2aの取得
セッション鍵Ks2bの生成
S36
S38
CRL番号のCRLからCRLdateを取得
S40
Ks2b、KPmc8とCRLdateをKs2aにて暗号化し、
[Ks2b/KPmc8/CRLdate]Ks2aの出力
S42
[Ks2b//KPmc8//CRLdate]Ks2eをKs2eにて復号し、
Ks2b、KPmc8およびCRLdateの受理
トランザクションID(b、コンテンツID(b、Kb、ACmbとACpbをKPmc8にて暗号化し、
(トランザクションID(b//コンテンツID(b//Kb//ACmb//ACpb)Kmc8の生成
S44
S48へ

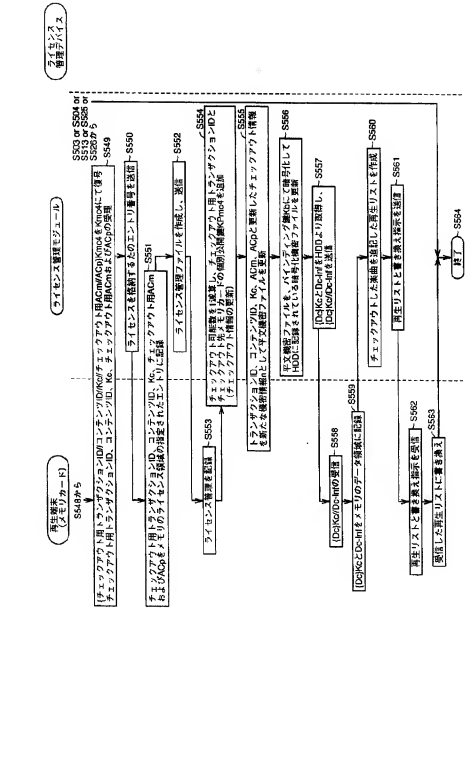
【図３２】


再生端末（メモリカード）
ライセンス管理モジュール
ライセンス管理デバイス
S524から
S525
KPmid0の有無
No
Yes
S526
Cm3 @ CRL
No
Yes
S551へ
S551
チェックアウト用トランザクションID(KCdb)Km3の受信
S552
KCdb)Km3を受け取り、Kcdb'の生成
S553
セッション鍵Kcdb'の生成
S554
CRL領域のCRL.dateをKCdb'に暗号化し、
S555
Kcdb'、KPmid、CRL.date をKCdb'にて暗号化し、
(KCdb)KPmid)(KCdb)CRL.date)(KCdb)Kcdb'の送信
チェックアウト用トランザクションID(KCdb)Km3の生成
S527
セッション鍵Kcdbの生成
S528
KPmidにてKcdbを暗号化し、(Kcdb)Km3の生成
S529
チェックアウト用トランザクションID(KCdb)Km3の送信
S530
(KCdb)KPmid)CRL.date)Kcdbを受信
S536
S537
(KCdb)KPmid)CRL.date)Kcdb をKCdbにて復号し、
Kcdb'、KPmidおよびCRL.dateの保管
S538
メモリカード内からKPmidおよびCRL.dateを読み出し、
メモリカード内のKPmidおよびCRL.dateを更新
S539へ
ライセンス管理デバイスへライセンス
移動/複製するKcdbを新たに生成し、ライセンス用ACnt生成

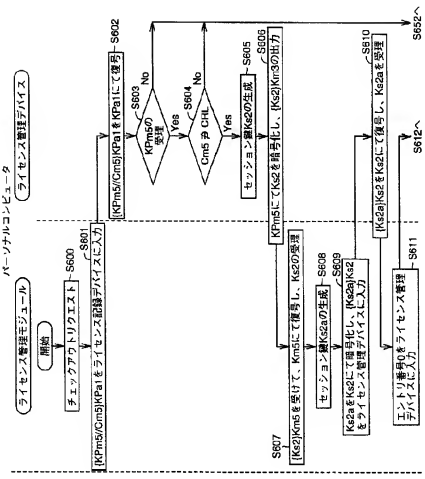
【図３３】


再生端末（メモリカード）
ライセンス管理モジュール
ライセンス管理デバイス
S538から
S539
チェックアウト用トランザクションID、コンテンツID、Kc、
Kcを暗号化するための鍵情報(Kcd)、
(チェックアウト用トランザクションID)/(コンテンツID)/(Kcd)/チェックアウト用ACm/ACp)Kmc4を生成
S540
CRLdate
新しいか？
No
Yes
S541
(チェックアウト用トランザクションID)/(コンテンツID)/(Kcd)/チェックアウト用ACm/ACp)Kmc4をKc2dに て暗号化し、
(チェックアウト用トランザクションID)/(Kcd)/チェックアウト用ACm/ACp)Kmc4)Kc2dの送信
(チェックアウト用トランザクションID)/(コンテンツID)/(Kcd)/チェックアウト用ACm/ACp)Kmc4)Kc2dの受信
S542
(チェックアウト用トランザクションID)/(コンテンツID)/(Kcd)/チェックアウト用ACm/ACp)Kmc4をKc2dにて復号
S543
S544
コンテンツ管理モジュール：実機のCRLをHDDより取得
(チェックアウト用トランザクションID)/(コンテンツID)/(Kcd)/チェックアウト用ACm/ACp)Kmc4をKc2dにて暗号化し、
(CRL)/(チェックアウト用トランザクションID)/(コンテンツID)/(Kcd)/チェックアウト用ACm/ACp)Kmc4)Kc2dの送信
S545
(CRL)/(チェックアウト用トランザクションID)/(コンテンツID)/(Kcd)/チェックアウト用ACm/ACp)Kmc4)Kc2dの受信
S546
(CRL)/(チェックアウト用トランザクションID)/(コンテンツID)/(Kcd)/チェックアウト用ACm/ACp)Kmc4)Kc2dにて復号
S547
CRLとチェックアウト用トランザクションID/(Kcd)/チェックアウト用ACm/ACp)Kmc4の受信
CRL差分のCRLを保存しCRLに書き換える
S548
S549へ

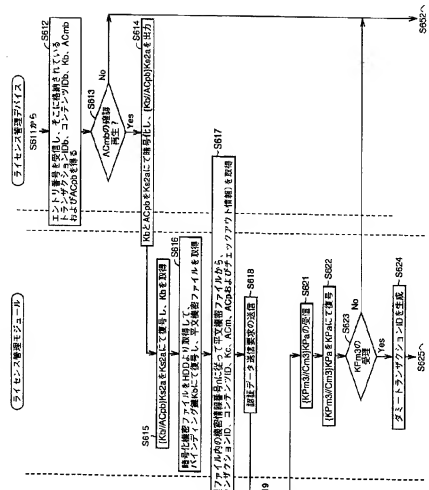
【図３４】


再生開始
（メディアカード）
S5484
ライセンス管理デバイス
ライセンス管理モジュール
S553
S554
S555
S556
S557
S558
S559
S560
S561
S562
S563
S564
終了

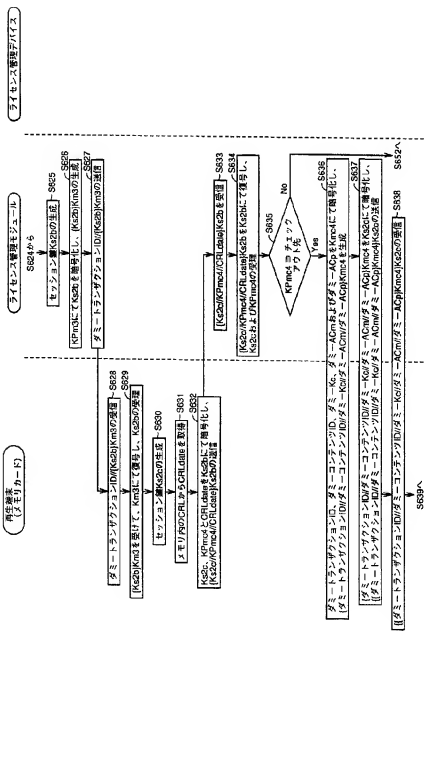
【図３５】


再生端末
（メモリカード）
パーソナルコンピュータ
ライセンス管理モジュール
ライセンス管理デバイス
開始
チェックアウトリクエスト
S600
S601
[KPm5i/Cm5i]KPa1をライセンス記録デバイスに入力
[KPm5i/Cm5i]KPa1をKPa1cで復号
S602
KPm5iの受理
S603
No
Yes
Cm5 = CHK
S604
No
Yes
セッション鍵Ks2の生成
S605
S606
KPm5にてKs2を暗号化し、[Ks2]Km3iの出力
S607
[Ks2]Km5を受けて、Km5cにて復号し、Ks2の受理
セッション鍵Ks2aの生成
S608
S609
Ks2aをKs2にて暗号化し、[Ks2a]Ks2をライセンス管理デバイスに入力
[Ks2a]Ks2をKs2cにて復号し、Ks2aを受理
S610
エントリ番号のみライセンス管理デバイスに入力
S611
S612へ
S692へ

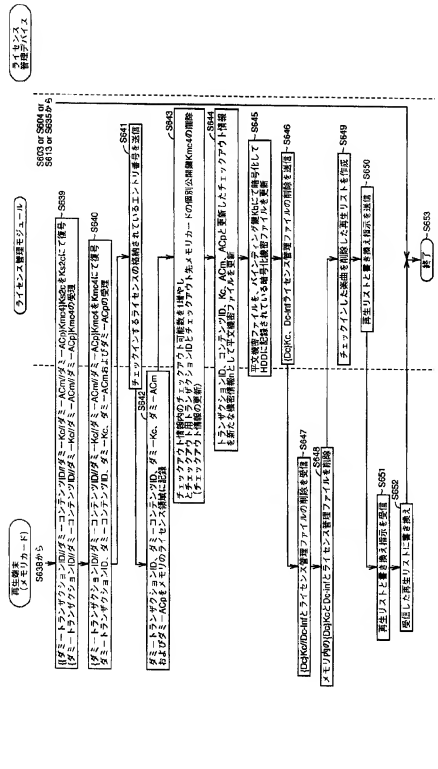
【図３６】


携帯端末（メモリカード）
ライセンス管理モジュール
ライセンス管理デバイス
S811から
エントリ番号が同じ、かつ未に無効とされている、トランザクションID、コンテンツID、Ko、ACmおよびACpbを得る
S812
ACmbの検証
No
Yes
S813
S814
Kb,とACpbをKeaIに渡し、{Ko}ACpbkeaを得る
S815
{Ko}ACpbKeaをKeaIに渡して復号し、Koを取得
S816
携帯端末アプリケーションに対して、Ko取得ファイルを取得
ライセンス管理ファイル内の属性情報番号に従って中文属性ファイルから、属性情報とトランザクションID、Kc、ACm、ACpbおよびチェックアウト情報を取得
S817
S818
課金データ送信要求の送信
S819
S820
{KPm3}KmSKPp送信
S821
{KPm3}KmSKPpを受信
S822
{KPm3}KmSKPpを{KPm3}Kmで復号
S823
KPm3の受理
No
Yes
S824
ダミートランザクションIDを生成
S825
S802

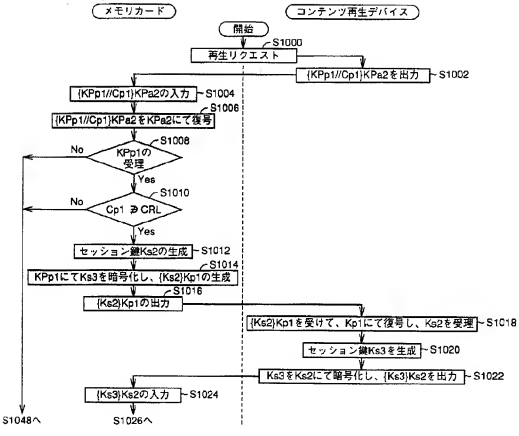
【図３７】


ライセンス管理デバイス
ライセンス管理モジュール
再生端末（メモリカード）
S824から
セッション鍵Kc2bの生成
S825
S826
S827
S828
S829
S830
S831
S832
S833
S834
S835
No
Yes
S836
S837
S838
S839へ
S832へ

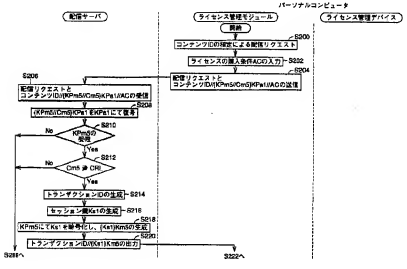
【図３８】


再生装置
(ユーザカード)
S639から
ライセンス管理モジュール
ライセンス
管理デバイス
S603 or S604 or
S613 or S635から
ダミートランザクションID/ダミーコンテンツID/ダミーKcd/ダミーACm/ダミーACnt/KcdをKcbにて復号
S639
ダミートランザクションID/ダミーコンテンツID/ダミーKcd/ダミーACnt/ダミーACplからKmcにて復号
S640
ダミートランザクションID、ダミーコンテンツID、ダミーKcd/ダミーACnt/ダミーACplからKmcにて復号
S641
(チェックインするライセンスの格納されているエントリ番号を返却
S642
ダミートランザクションID、ダミーコンテンツID、ダミーKc、ダミーACm
S643
およびダミーACpをメモリのライセンス領域に記録
(チェックアウト情報のチェックアウト可能数を1減やし、
チェックアウトトランザクションIDとチェックアウト先メモリカードの情報(公開鍵Kmc)の削除
(チェックアウト情報の更新)
S644
トランザクションID、コンテンツID、Kc、ACm、ACplに基づいたチェックアウト情報
を新たな情報格納エリアとして子文書署名ファイルを更新
S645
子文書署名ファイルをメモリカードから読み出して
HDD記録されている親文書署名ファイルを更新
DcKc、DcmライセンスDB管理ファイルを復号
S646
DcKc/DcmとライセンスDB管理ファイルの整合を検証
S647
メモリ内のDcKcとDcmにてライセンス管理ファイルを再暗号
S648
チェックインした楽曲を削除した再生リストを作成
S649
再生リストと署名情報を表示
S650
再生リストと署名情報を保存
S651
保存した再生リストに署名を添付
S652
終了
S653

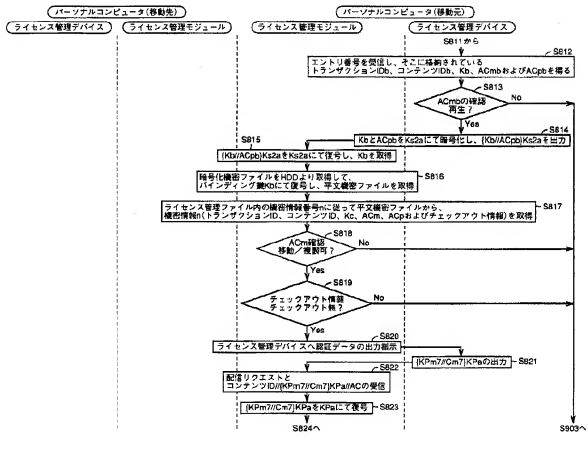
【図３９】


メモリカード
コンテンツ再生デバイス
開始
S1000
再生リクエスト
{KPp1//Cp1}KPa2を出力
S1002
{KPp1//Cp1}KPa2の入力
S1004
S1006
{KPp1//Cp1}KPa2をKPa2にて復号
S1008
No
KPp1の受理
Yes
S1010
No
Cp1 ≠ CRL
Yes
セッション鍵Ks2の生成
S1012
S1014
KPp1にてKs3を暗号化し、{Ks2}Kp1の生成
S1016
{Ks2}Kp1の出力
{Ks2}Kp1を受けて、Kp1にて復号し、Ks2を受理
S1018
セッション鍵Ks3を生成
S1020
Ks3をKs2にて暗号化し、{Ks3}Ks2を出力
S1022
{Ks3}Ks2の入力
S1024
S1048へ
S1026へ

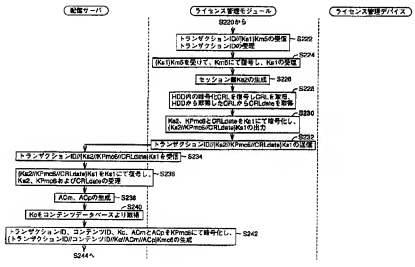
【図５３】


パーソナルコンピュータ
配信サーバ
ライセンス管理モジュール
ライセンス管理デバイス
開始
S200
コンテンツIDの指定による配信リクエスト
ライセンスの購入条件ACの入力
S202
S204
配信リクエストと
コンテンツID{K(KPms5/Cms5(KPa1)AC}の送信
S206
配信リクエストと
コンテンツID{K(KPms5/Cms5(KPa1)AC}の受信
S208
{KPms5/Cms5}KPa1 KPp1にて復号
S210
No
KPms5の受理
Yes
S212
No
Cms ≠ CRL
Yes
トランザクションIDの生成
S214
セッション鍵Ks1の生成
S216
S218
{KPms5にてKs1を暗号化し、{Ks1}KMs5の生成
S220
トランザクションID{K(Ks1)KMs5}の出力
S208へ
S222へ

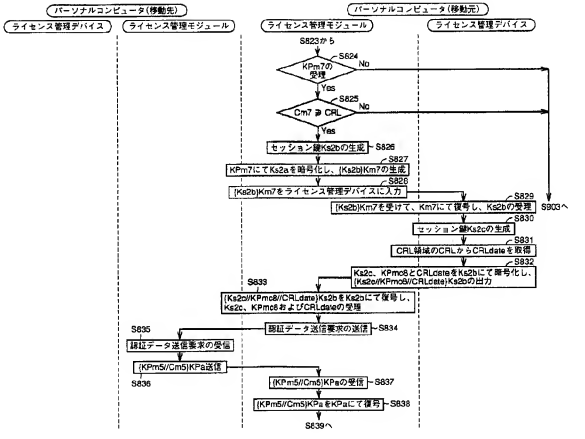
【図４２】


パーソナルコンピュータ（移動先）
ライセンス管理デバイス
ライセンス管理モジュール
パーソナルコンピュータ（移動元）
ライセンス管理モジュール
ライセンス管理デバイス
S811から
S812
エントリ番号を頼信し、そこに格納されている
トランザクションIDb、コンテンツIDb、Kb、ACmbおよびACpbを得る
S813
ACmbの検証
再生？
No
Yes
S814
KbとACpbをKs2aにて暗号化し、{Kb/ACpb}Ks2aを出力
S815
{Kb/ACpb}Ks2aをKs2aにて復号し、Kbを取得
S816
暗号化機密ファイルをHDDより取得して、
バインディング鍵Kbにて復号し、平文機密ファイルを取得
S817
ライセンス管理ファイル内の機密情報番号mに従って平文機密ファイルから、
機密情報{トランザクションID、コンテンツID、Kc、ACm、ACpおよびチェックアウト情報}を取得
S818
ACm検証
移動／複製可？
No
Yes
S819
チェックアウト情報
チェックアウト時？
No
Yes
S820
ライセンス管理デバイスへ認証データの出力指示
{KPm7//Cm7}KPaの出力
S821
S822
配信リクエストと
コンテンツID//{KPm7//Cm7}KPa//ACの受信
{KPm7//Cm7}KPaをKPaにて復号
S823
S824へ
S903へ

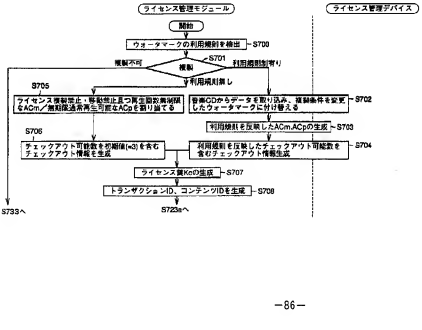
【図５４】


配信サーバ
ライセンス管理モジュール
ライセンス管理デバイス
S220から
トランザクションID//Ks1//Kmsの復信
トランザクションID//Kmsの受理
S232
S234
{Ks1}Kmsを受けて、Kmsにて復号し、Ks1の受理
セッション鍵Ks2の生成
S236
S238
HDD内の暗号化CRLを復号しCRLを管理
HDDから新規なCRLかSCRLsetを取得
S240
Ks2、KPmsdとCRLsetをKs1にて暗号化し、
{Ks2//KPmsd//CRLset}Ks1の出力
S242
トランザクションID//{Ks2//KPmsd//CRLset}Ks1の出力
トランザクションID//{Ks2//KPmsd//CRLset}Ks1を受信
S234
{Ks2//KPmsd//CRLset}Ks1をKs1にて復号し、
Ks2、KPmsdおよびCRLsetの受理
S236
ACm、ACpの生成
S238
S240
KsをコンテンツデータベースよりS242
トランザクションID、コンテンツID、Kc、ACmとACpをKPmsdにて暗号化し、
{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmsdの生成
S242
S244へ

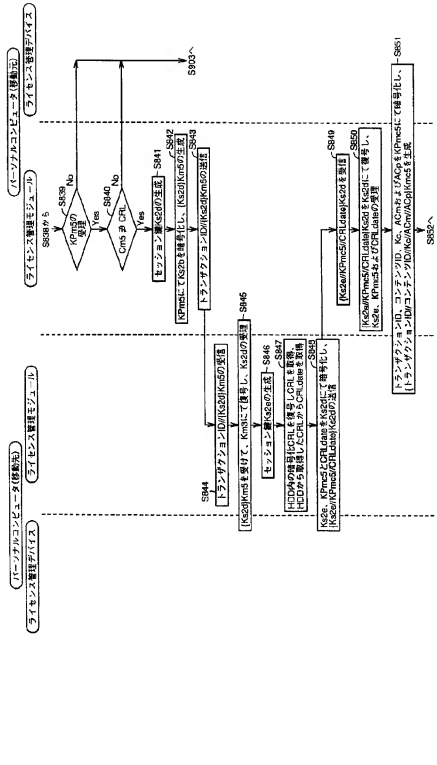
【図４３】

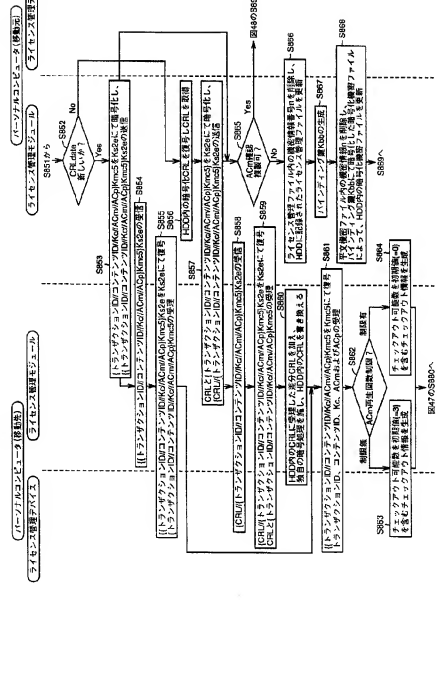

パーソナルコンピュータ(移動先)
パーソナルコンピュータ(移動元)
ライセンス管理デバイス
ライセンス管理モジュール
ライセンス管理モジュール
ライセンス管理デバイス
S823から
S824
KPm7の受理
No
Yes
S825
Cm7 ∋ CRL
No
Yes
セッション鍵Ks2bの生成
S826
S827
KPm7にてKs2aを暗号化し、{Ks2b|Km7}の生成
S828
{Ks2b|Km7}をライセンス管理デバイスに入力
S829
{Ks2b|Km7}を受けて、Km7にて復号し、Ks2bの受理
S903へ
S830
セッション鍵Ks2cの生成
S831
CRL領域のCRLからCRLdateを取得
S832
Ks2c、KPmc8とCRLdateをKs2bにて暗号化し、{Ks2c/KPmc8/CRLdate}Ks2bの出力
S833
{Ks2c/KPmc8/CRLdate}Ks2bをKs2bにて復号し、Ks2c、KPmc8およびCRLdateの受理
S835
認証データ送信要求の受信
認証データ送信要求の送信
S834
{KPm5/Cm5}KPa送信
S836
{KPm5/Cm5}KPaの受信
S837
{KPm5/Cm5}KPaをKPaにて復号
S838
S839へ

【図５７】


ライセンス管理モジュール
ライセンス管理デバイス
開始
ウォータマークの利用規則を検出
S700
S701
複数
利用規則指定有り
複製不可
利用規則無し
S705
ライセンス複製禁止・転送禁止及び再生回数無制限をACm/無利用規則を含まないACbを割り当てる
音楽CDからデータを取り込み、複製条件を変更したウォータマークに付け替える
S702
利用規則を反映したACm,ACpの生成
S703
S706
チェックアウト可能数を初期値(=3)を含むチェックアウト情報を生成
利用規則を反映したチェックアウト可能数を含むチェックアウト情報生成
S704
ライセンス鍵Kcの生成
S707
トランザクションID、コンテンツIDを生成
S708
S733へ
S723aへ

【図４４】

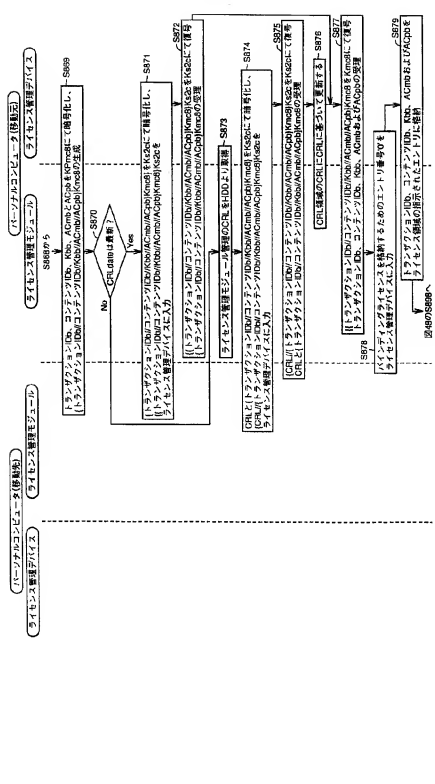

パーソナルコンピュータ(移動元)
ライセンス管理デバイス
ライセンス管理モジュール
パーソナルコンピュータ(移動先)
ライセンス管理モジュール
ライセンス管理デバイス
S838
S839
S840
S841
S842
S843
S844
S845
S846
S847
S848
S849
S850
S851
S852
S903
No
Yes
No
Yes
セッション鍵Kcdの生成
KPmsiにKcdを暗号化し、[Kcd]Kcmsiの生成
トランザクションID//[Kcd]Kcmsiの送信
トランザクションID//[Kcd]Kcmsiの受信
[Kcd]Kcmsiを受け取り、Kcmsiにて復号し、Kcdの取得
セッション鍵Kcdの生成
HDDAの時刻をCRLと照合、HDDからCRLdateを取得
Kcd、KPmsiよりCRLdateを[Kcd]KPmsiにて暗号化し、[Kcd]KPmsiをCRLdateに付加
[Kcd]KPmsi+[CRLdate]Kcdを復号
[Kcd]KPmsi+[CRLdate]Kcdを[Kcd]KPmsiにて復号し、Kcd、KPmsiおよびCRLdateの取得
[Kcd]KPmsi+[CRLdate]Kcdを[Kcd]KPmsiにて暗号化し、
[Kcd]KPmsi+[CRLdate]Kcdを生成
トランザクションID、Kc、ACmおよびACpを[Kcd]KPmsiにて暗号化し、
[トランザクションID//コンテンツID//Kc//ACm//ACp]KPmsiを生成
KPmsi=?
Kcd=?
KPmsi=?
Cms ≧ CRL
KPmsi=?
Kcd=?



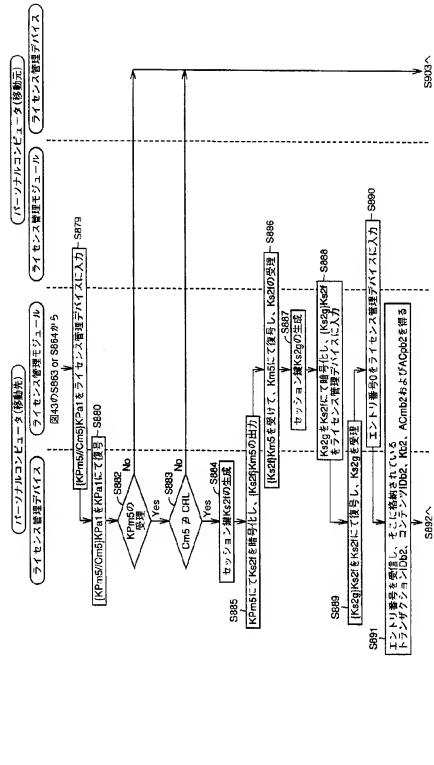
【図４５】

パーソナルコンピュータ（移動先）
ライセンス管理デバイス
ライセンス管理モジュール
パーソナルコンピュータ（移動元）
ライセンス管理モジュール
ライセンス管理デバイス
S851から
S852
CRLdate
新しいか？
No
Yes
S853
{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc5をKs2eにて暗号化し、
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc5}Ks2eの送信
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc5}Ks2eの受信
S854
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc5}Ks2eをKs2eにて復号
{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc5の受理
S855
S856
HDD内の暗号化CRLを復号しCRLを取得
S857
CRLと{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc5}をKs2eにて暗号化し、
{CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc5}Ks2eの送信
{CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc5}Ks2eの受信
S858
{CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc5}Ks2eをKs2eにて復号
CRLと{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc5の受理
S859
S860
HDD内のCRLに受理した差分CRLを加え、
独自の暗号処理を施し、HDD内のCRLを書き換える
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc5をKmc5にて復号
トランザクションID、コンテンツID、Kc、ACmおよびACpの受理
S861
S862
ACm再生回数制限？
制限無
制限有
S863
チェックアウト可能数を初期値(=3)
を含むチェックアウト情報を生成
S864
チェックアウト可能数を初期値(=0)
を含むチェックアウト情報を生成
図47のS880へ
S865
ACm確認
複製可？
Yes
図48のS898へ
No
ライセンス管理ファイル内の機密情報番号nを削除し、
HDDに記録されたライセンス管理ファイルを更新
S866
バインディング鍵Kbbの生成
S867
平文機密ファイル内の機密情報nを削除し、
バインディング鍵Kbbにて暗号化した暗号化機密ファイル
によって、HDD内の暗号化機密ファイルを更新
S868
S869へ

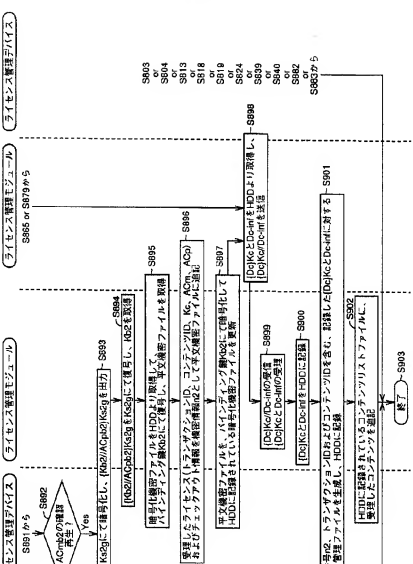
【図４６】


パーソナルコンピュータ(依頼元)
ライセンス管理デバイス
ライセンス管理モジュール
パーソナルコンピュータ(依頼先)
ライセンス管理モジュール
ライセンス管理デバイス
S869から
S869
S870
CRLdata14 異常 ?
No
Yes
S871
S872
S873
S874
S875
S876
S877
S878
S879
S880へ

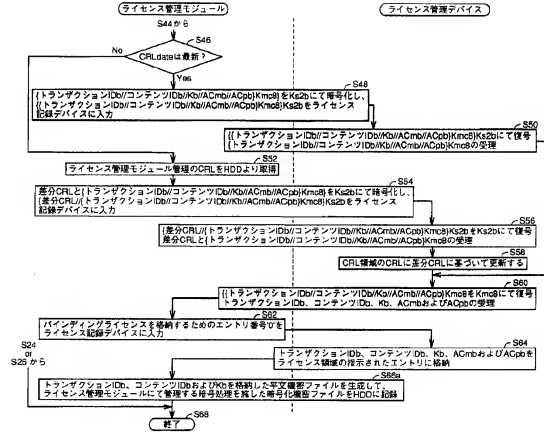
【図４７】


パーソナルコンピュータ(移動先)
ライセンス管理デバイス
ライセンス管理モジュール
パーソナルコンピュータ(移動元)
ライセンス管理モジュール
ライセンス管理デバイス
図437のS863 or S864から
[KPmb/Cm5]KPa1をライセンス管理デバイスに入力
S879
[KPm5/Cm5]KPa1をKPa1にて復号
S880
KPa1の整合
S882
No
Yes
Cm5 ≠ CHL
S883
No
Yes
セッション鍵Ks2sの生成
S884
S885
[Ks2s]Km5のKm5出力
[Ks2s]Km5にてKs2sを暗号化し、
[Ks2s]Km5を受けて、Km5にて復号し、Ks2sの受理
S886
セッション鍵Ks2g の生成
S887
Ks2gをKs2sにて暗号化し、[Ks2g]Ks2sをライセンス管理デバイスに入力
S888
S889
[Ks2g]Ks2sをKs2sにて復号し、Ks2gを受理
S891
エントリ番号Sをライセンス管理デバイスに入力
S890
エントリ番号Sを受信し、さらに格納されている
トランザクションIDb2、コンテンツIDb2、Kt2、ACmb2およびACpb2を得る
S892へ
S893へ

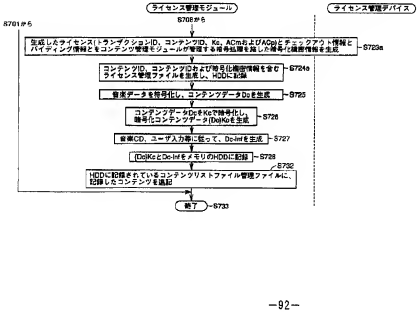
【図４８】


パーソナルコンピュータ（移動元）
ライセンス管理デバイス
ライセンス管理モジュール
パーソナルコンピュータ（移動先）
ライセンス管理デバイス
S893 から
S892
No
ACmb2の複製再生？
Yes
S893
Kb2とACpk2をKs3gにて復号化し、{Kb2//ACpk2}Ks3gをHDに記録
S894
{Kb2//ACpk2}Ks3gをKs3gにて再号し、Kb2を取得
S895
属性化暗号ファイルをHDから取得して、ライセンス属性Kcにて復号し、平文属性ファイルを取得
S896
管理したライセンス（トランザクションID、コンテンツID、Kc、ACm、ACb）およびチェックアウト情報を暗号属性情報2として平文属性ファイルに追記
S897
平文属性ファイルを、パイプリング暗号2Kにて暗号化して、Kcにて属性化された暗号属性ファイルを更新
S898
[DcIKc:Dc-ariを]HDより取得し、[DcIKc:Dc-ariを]送信
S899
[DcIKc:Dc-inf0の受信][DcIKc:Dc-inf0の受理]
S900
[DcIKc:Dc-arifを]HDに記録
S901
属性情報番号n2、トランザクションIDおよびコンテンツIDを含む、記録した[DcIKc:Dc-arif]に対するライセンス管理ファイルを生成し、HDに記録
S902
有効に記録されているコンテンツリストファイル、管理したライセンスを選択
S903
終了
S903 or S879から
S903
or
S904
or
S913
or
S918
or
S919
or
S924
or
S939
or
S940
or
S941
S982
S983
から

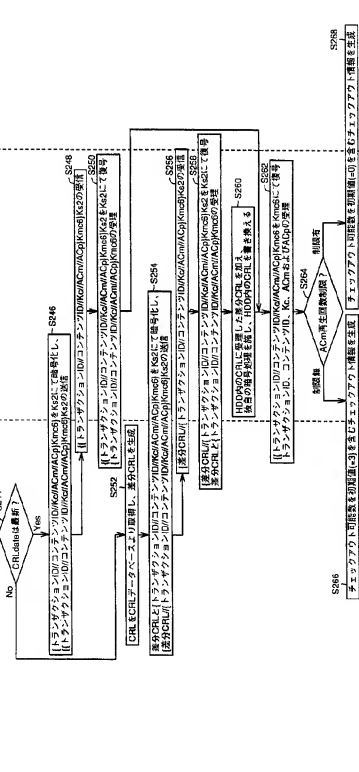
【図５２】


ライセンス管理モジュール
ライセンス管理デバイス
S44から
S45
No
CRLdateは最新？
Yes
S48
{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8をKs2bにて暗号化し、
{{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8}Ks2bをライセンス
記録デバイスに入力
S50
{{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8}Ks2bにて復号
{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8の受理
S52
ライセンス管理モジュール管理のCRLをHDDより取得
S54
差分CRLと{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8をKs2bにて暗号化し、
{差分CRLと{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8}Ks2bをライセンス
記録デバイスに入力
S56
{差分CRLと{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8}Ks2bをKs2bにて復号
差分CRLと{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8の受理
S58
CRL領域のCRLに差分CRLに基づいて更新する
S60
{{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8をKmc8にて復号
トランザクションIDb、コンテンツIDb、Kb、ACmbおよびACpbの受理
S62
バインディングライセンスを格納するためのエントリ番号Uを
ライセンス記録デバイスに入力
S24
or
S25から
S64
トランザクションIDb、コンテンツIDb、Kb、ACmbおよびACpbを
ライセンス領域の指示されたエントリに格納
S66a
トランザクションIDb、コンテンツIDbおよびKbを格納した平文構造ファイルを生成して、
ライセンス管理モジュールにて管理する暗号処理を施した暗号化構造ファイルをHDDに記録
S68
終了

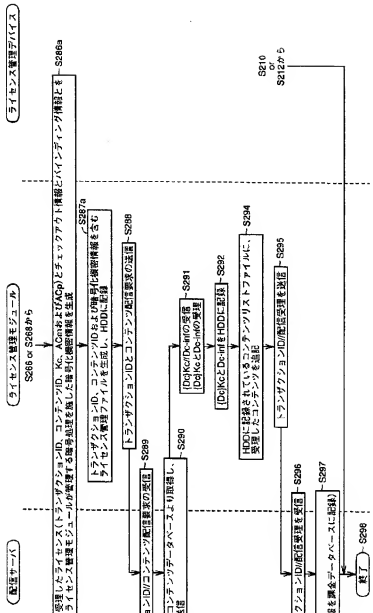
【図５８】


ライセンス管理モジュール
ライセンス管理デバイス
S701から
S708から
生成したライセンス{トランザクションID、コンテンツID、Ks、ACmbおよびACpbとチェックアウト情報と
バインディング情報とをコンテンツ管理モジュールが管理する暗号処理を施した暗号化構造情報を生成
S723a
コンテンツID、コンテンツ鍵および暗号化構造情報を含む
ライセンス管理ファイルを生成し、HDDに記録
S724a
音楽データを符号化し、コンテンツデータDcを生成
S725
コンテンツデータDcをKcで暗号化し
暗号化コンテンツデータ{Dc}Kcを生成
S726
音楽CD、ユーザ入力等に従って、Dc.infを生成
S727
{Dc}KcとDc.infをメモリ内のHDDに記録
S728
S732
HDDに記録されているコンテンツリストファイル管理ファイルに、
記録したコンテンツを追記
終了
S733

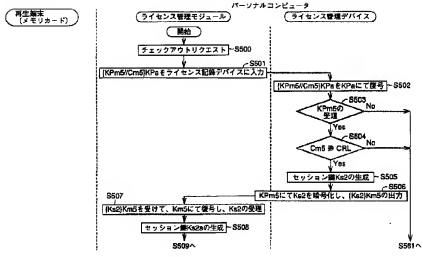
【図５５】


配信サーバ
ライセンス管理モジュール
ライセンス管理デバイス
S242から
S244
CRLdataは最新？
No
Yes
S246
S248
S250
S252
CRLをCRLデータベースより取得し、差分CRLを生成
S254
S256
S258
S260
S262
S264
S266
S266aへ
初期時
AUth再生回数残数？
AUth再生回数を初期値(=0)をまたはチェックアウト情報を生成

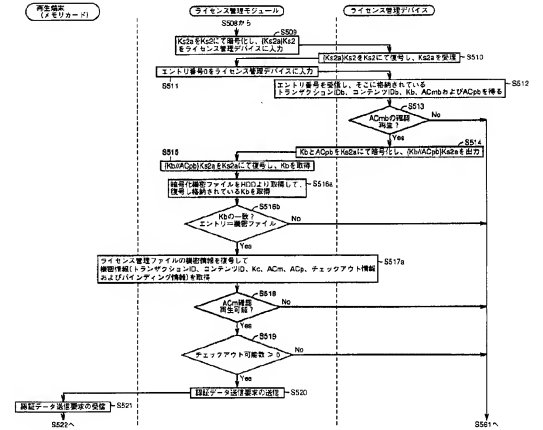
【図５６】


配信サーバ
ライセンス管理デバイス
ライセンス管理をモジュール
S286 or S288から
受理したライセンス（トランザクションID、Kc、ACcおよびAD(p)とチェックアウト情報とバインディング情報とを含むライセンス管理モジュールが発行する端末固有な暗号化鍵情報を含む）
S286a
S287a
トランザクションID、コンテンツIDおよび暗号化鍵情報を含む
ライセンス管理ファイルを生成し、HDDに記録
トランザクションIDとコンテンツ配信要求の送信
S288
トランザクションID/コンテンツ配信要求の受信
S289
Dc|Kc|Dc-inf|をコンテンツデータベースより読み出し、
S290
|Dc|Kc|Dc-inf|の受信
|Dc|Kc|Dc-inf|を記録
S291
|Dc|Kc|Dc-inf|をHDDに記録
S292
HDDに記録されているコンテンツリストファイルに、受理したコンテンツを追記
S294
S210
or
S212から
トランザクションID/配信受理情報を送信
S295
トランザクションID/配信要求情報を受信
S296
課金処理
（課金情報をデータベースに記録）
S297
終了
S298

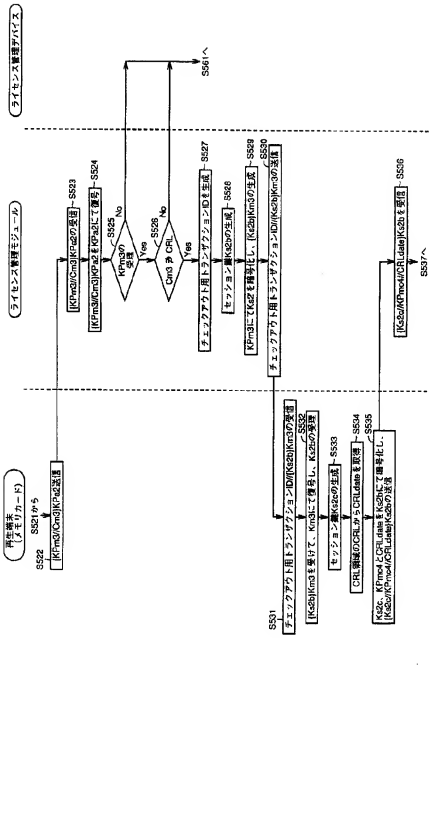
【図５９】


再生端末
(メモリカード)
パーソナルコンピュータ
ライセンス管理モジュール
ライセンス管理デバイス
開始
チェックアウトリクエスト
S500
S501
[KPm5/Cm5]KPaをライセンス記録デバイスに入力
[KPm5/Cm5]KPaをKPaにて復号
S502
S503
KPm5の一致
No
Yes
S504
Cm5 ∋ CRL
No
Yes
セッション鍵Ks2の生成
S505
S506
KPm5にてKs2を暗号化し、[Ks2]Km5の出力
S507
[Ks2]Km5を受け取り、Km5にて復号し、Ks2の受理
セッション鍵Ks2aの生成
S508
S509へ
S561へ

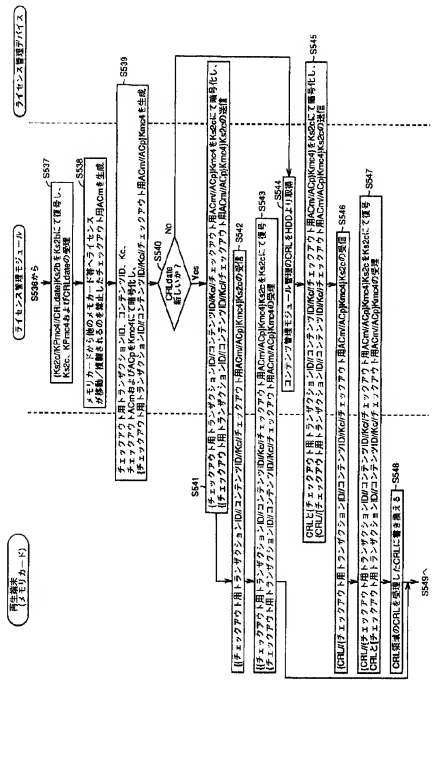
【図６０】


再生端末
(メモリカード)
ライセンス管理モジュール
ライセンス管理デバイス
S508から
S509
Ks2aをKs2にて暗号化し、[Ks2a]Ks2
をライセンス管理デバイスに入力
[Ks2a]Ks2をKs2にて復号し、Ks2aを受理
S510
エントリ番号をライセンス管理デバイスに入力
S511
エントリ番号を受信し、そこに格納されている
トランザクションID、コンテンツID、Kb、ACmbおよびACpbを得る
S512
S513
ACmbの検証
再度？
No
Yes
S514
S515
KbとACpbをKs2aにて暗号化し、(Kb/ACpb)Ks2aを出力
(Kb/ACpb)Ks2aをKs2aにて復号し、Kbを取得
暗号化鍵ファイルをHDDより取得して、
復号し格納されているKbを取得
S516a
S516b
Kbの一致？
エントリ=鍵ファイル
No
Yes
ライセンス管理ファイルの鍵情報を復号して、
鍵情報(トランザクションID、コンテンツID、Kc、ACm、ACp、チェックアウト情報
およびバインディング情報)を取得
S517a
S518
ACmの検証
再度？
No
Yes
S519
チェックアウト可能数 > 0
No
Yes
課金データ送信要求の送信
S520
課金データ送信要求の受信
S521
S522へ
S561へ

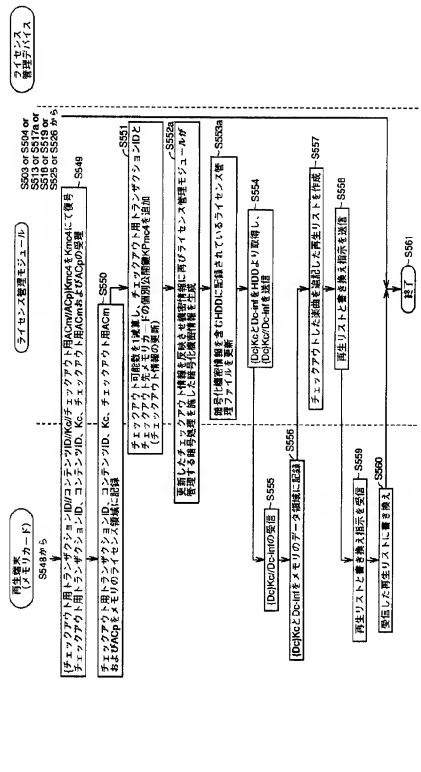
【図６１】


再生端末（メモリカード）
ライセンス管理モジュール
ライセンス管理デバイス
S522
S521から
Kfmd0/Cmd0/KPad送信
S523
KPmd0/Cmd0/KPadの受信
S524
KPmd0/Cmd0/KPadとKPpdcに「復号」
S525
KPmd0の受信
No
Yes
S526
Cmd3 or CRL
No
Yes
S501へ
S527
チェックアウト用トランザクションIDを生成
S528
「セッション鍵Kdbの生成」
S529
KPmdに「Kdb」を暗号化し、{Kdb}Kmd0の生成
S530
チェックアウト用トランザクションID//{Kdb}Kmd0の送信
S531
チェックアウト用トランザクションID//{Kdb}Kmd0の受信
S532
{Kdb}Kmdを受け取り、Kmdにて復号し、Kdbの受信
S533
セッション鍵Kdbの生成
S534
CRL領域のCRLカウンタの読取
S535
Kdb、KPmdよりCRLdateを暗号化し、{Kdb//KPmd//CRLdate}Kdb0の生成
S536
{Kdb//KPmd//CRLdate}Kdb0を送信
S537へ

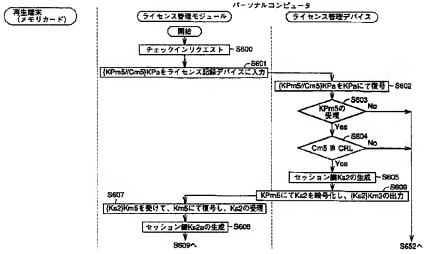
【図６２】


再生装置（メモリカード）
ライセンス管理モジュール
ライセンス管理デバイス
S536から
KCdc,Nm'mc4,URLdata,KCdc'をKCdcにて復号し、
S537
KCdc,Nmc4よりURLdataの受理
S538
メモリカードから鍵のメモカ－ド等へライセンス
が移動／複製されるのを禁止したチェックアウト用ACmを生成
S539
チェックアウト用トランザクションID、コンテンツID、Kc、
チェックアウトACmおよびAcpをKmc4にて暗号化し、
チェックアウト用トランザクションIDのコンテンツID用のチェックアウト用ACmのAcpをKmc4を生成
S540
CRL情報
新しい？
No
Yes
S541
チェックアウト用トランザクションID/コンテンツID用のチェックアウト用ACmのAcpをKmc4をKcdcにて暗号化し、
チェックアウト用トランザクションID/コンテンツID用のチェックアウト用ACmのAcpの送信
S542
チェックアウト用トランザクションID/コンテンツID用のチェックアウト用ACmのAcpをKmc4をKcdcにて復号
S543
コンテンツ管理モジュール管理のCRLをHDD上に記録
S544
CRLリチェックアウト用トランザクションID/コンテンツID用のチェックアウト用ACmのAcpをKmc4をKcdcにて暗号化し、
CRLリチェックアウト用トランザクションID/コンテンツID用のチェックアウト用ACmのAcpの送信
S545
CRLリチェックアウト用トランザクションID/コンテンツID用のチェックアウト用ACmのAcpをKmc4をKcdcにて復号
S546
CRLリチェックアウト用トランザクションID/コンテンツID用のチェックアウト用ACmのAcpをKmc4をKcdcにて暗号
CRLとチェックアウト用トランザクションID/コンテンツID用のチェックアウト用ACmのAcpの送信
S547
CRL鍵通のCRLを受理したCRLに書き換える
S548
S549へ

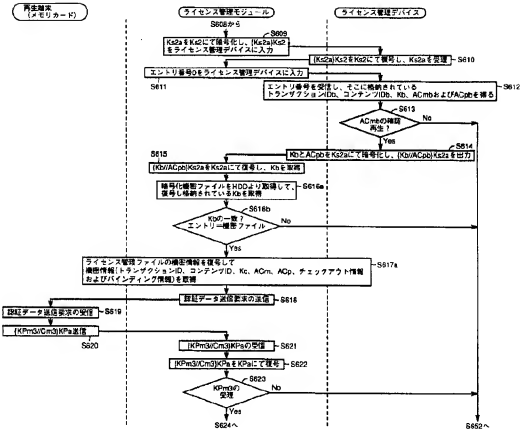
【図６３】


再生要求
(メモリカード)
S548から
ライセンス管理モジュール
ライセンス
管理デバイス
S503 or S504 or
S513 or S517a or
S516 or S519 or
S525 or S526 から
チェックアウト用トランザクションID/Kg/チェックアウト用Cont/Kp/Kmc4/Kmc4にて復号
チェックアウト用トランザクションID、コンテンツID、Kc、チェックアウト用ACont2およびACpp0を送信
S549
チェックアウト用トランザクションID、コンテンツID、Kc、チェックアウト用ACont
S550
チェックアウト可能数を1減算し、チェックアウト用トランザクションIDと
チェックアウトしたメモリカードの識別情報(Kmc4)を追加
(チェックアウト情報の更新)
S551
S552a
要求したチェックアウト情報と異なる場合は再度情報に再びライセンス管理モジュールが
管理する暗号処理を施した情報を生成する
S552b
暗号化機能付機器を含むHDDに記録されているライセンス等
管理ファイルを更新
S553a
[Dc]Kc/Dc-intの受信
S555
[Dc]Kc/Dc-intをメモリのデータ領域に記録
S556
[Dc]Kc/Dc-intの受信
S554
[Dc]Kc/Dc-intを送信
チェックアウトした楽曲を識別した再生リストを作成
S557
再生リストと書き換え指示を送信
S558
再生リストと書き換え指示を受信
S559
受信した再生リストに書き換え
S560
終了
S561

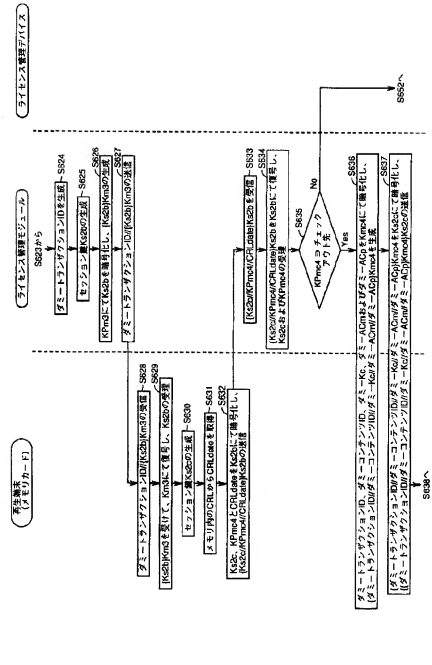
【図６４】

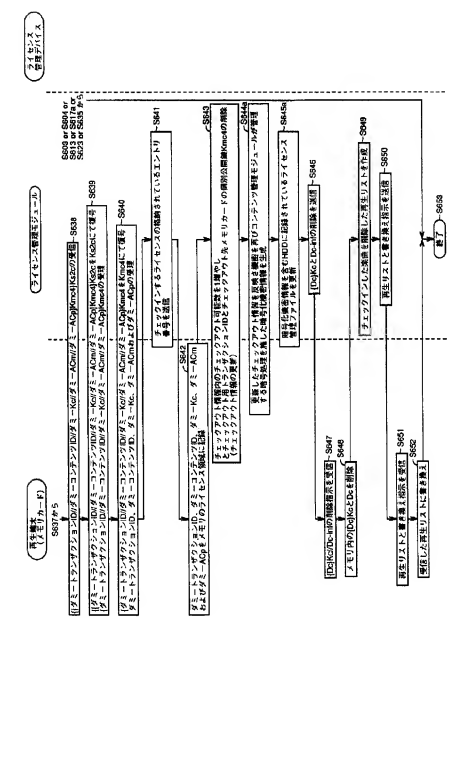

再生端末
(メモリカード)
パーソナルコンピュータ
ライセンス管理モジュール
ライセンス管理デバイス
開始
チェックインリクエスト
S600
S601
[KPms3/Cm3]KPaをライセンス記録デバイスに入力
[KPms5/Cm5]KPaをKPaにて復号
S602
KPms5の受理
S603
No
Yes
Cms5 = CHL
S604
No
Yes
セッション鍵Ks2の生成
S605
S606
KPms5にてKs2を暗号化し、[Ks2]Kms5の出力
S607
[Ks2]Kms5を受けて、Kms5にて復号し、Ks2の受理
セッション鍵Ks2aの生成
S608
S609へ
S652へ

【図６５】


再生端末
(メモリカード)
ライセンス管理モジュール
S606から
ライセンス管理デバイス
S609
Ks2aをKs2にて暗号化し、[Ks2a]Ks2をライセンス管理デバイスに入力
[Ks2a]Ks2をKs2にて復号し、Ks2aを受理
S610
エントリ番号をライセンス管理デバイスに入力
S611
エントリ番号を受信し、それに格納されているトランザクションID、コンテンツID、Kb、ACmbおよびACpbを読み
S612
S613
ACmbの検証
No
Yes
S614
S615
KbとACpbをKs2aにて暗号化し、[Kb/ACpb]Ks2aを出力
[Kb/ACpb]Ks2aをKs2aにて復号し、Kbを取得
暗号化機能ファイルをHDDより取得して、復号し格納されているKbを取得
S616a
Kbが一致？
エントリー機能ファイル
S616b
No
Yes
ライセンス管理ファイルの構成情報を復号して
構成情報(トランザクションID、コンテンツID、Kc、ACm、ACp、チェックアウト情報
およびバインディング情報)を取得
S617a
課金データ送信要求の送信
S616
課金データ送信要求の受信
S619
[KPms3/Cm3]KPa送信
S620
[KPms3/Cm3]KPaの受信
S621
[KPms3/Cm3]KPaをKPaにて復号
S622
KPmsの受理
S623
No
Yes
S624へ
S652へ

【図６６】

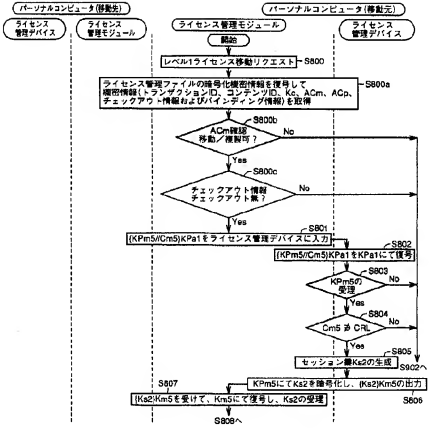

ライセンス管理デバイス
ライセンス管理モジュール
S823から
ダミートランザクションIDを生成 S824
セッション鍵Kcdbの生成 S825
KPmdにてKcdbを暗号化し、[Kcdb]Kmdの生成 S826
ダミートランザクション[ID][Kcdb]Kmdの送信 S827
S692へ
S828へ
ダミートランザクション[ID]、ダミーコンテンツID、ダミーKc、ダミーAUnitよりダミーAUp をKmdにて暗号化し、
ダミートランザクション[ID]ダミーコンテンツID[ダミーKcu]ダミーAUp[ダミーKmd]を送信
[ダミートランザクション[ID]ダミーコンテンツID[ダミーKcu]ダミーAUp[ダミーKmd]をKcdbにて暗号化し、
[ダミートランザクション[ID]ダミーコンテンツID[ダミーKcu]ダミーAUp[ダミーKmd]Kcdbの送信
S836
KPmcdヨチェック
アウト有
No
Yes
S835
[Kcdb]KPmcdにてCRLdateを暗号化し、
[Kcdb]KPmcd/CRLdate]Kcdbを送信 S833
[Kcdb]KPmcd/CRLdate]Kcdbを受信 S834
[Kcdb]KPmcd/CRLdate]Kcdbにて復号し、
Kcdbおよび KPmcdの抽出
メモリ内のCRLPからCRLdateを取得 S831
Kcdb、KPmcdとCRLdateをKcdbにて暗号化し、
[Kcdb]KPmcd/CRLdate]Kcdbの送信 S832
[Kcdb]Kmdを受けて、Kmdにて復号し、Kcdbの抽出
セッション鍵Kcdbの生成 S830
ダミートランザクション[ID][Kcdb]Kmdの受信 S829
S692へ



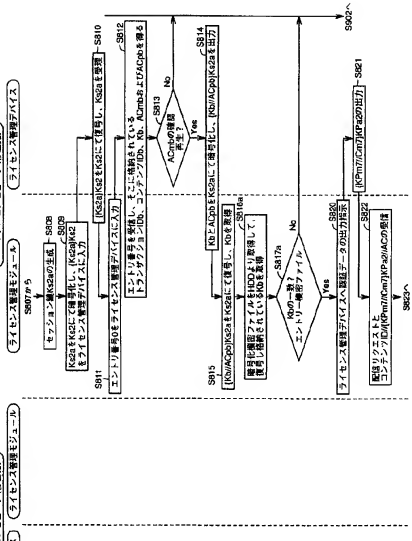
【図６７】

再生端末（メモリカード）
ライセンス管理モジュール
ライセンス管理デバイス
S637から
{{ダミートランザクションID//ダミーコンテンツID//ダミーKc//ダミーACm//ダミーACp}Kmc4}Ks2cの受信
S638
{{ダミートランザクションID//ダミーコンテンツID//ダミーKc//ダミーACm//ダミーACp}Kmc4}Ks2cをKs2cにて復号
{ダミートランザクションID//ダミーコンテンツID//ダミーKc//ダミーACm//ダミーACp}Kmc4の受理
S639
{ダミートランザクションID//ダミーコンテンツID//ダミーKc//ダミーACm//ダミーACp}Kmc4をKmc4にて復号
ダミートランザクションID、ダミーコンテンツID、ダミーKc、ダミーACmおよびダミーACpの受理
S640
S603 or S604 or
S613 or S617a or
S623 or S635 から
チェックインするライセンスの格納されているエントリ番号を送信
S641
S642
ダミートランザクションID、ダミーコンテンツID、ダミーKc、ダミーACmおよびダミーACpをメモリのライセンス領域に記録
S643
チェックアウト情報内のチェックアウト可能数を1増やし
とチェックアウト用トランザクションIDとチェックアウト先メモリカードの個別公開鍵Kmc4の削除
（チェックアウト情報の更新）
S644a
更新したチェックアウト情報を反映さ機密を再びコンテンツ管理モジュールが管理する暗号処理を施した暗号化機密情報を生成
暗号化機密情報を含むHDDに記録されているライセンス管理ファイルを更新
S645a
{Dc}KcとDc-infの削除を送信
S646
{Dc}Kc//Dc-infの削除指示を受信
S647
S648
メモリ内の{Dc}KcとDcを削除
チェックインした楽曲を削除した再生リストを作成
S649
再生リストと書き換え指示を送信
S650
再生リストと書き換え指示を受信
S651
S652
受信した再生リストに書き換え
終了
S653

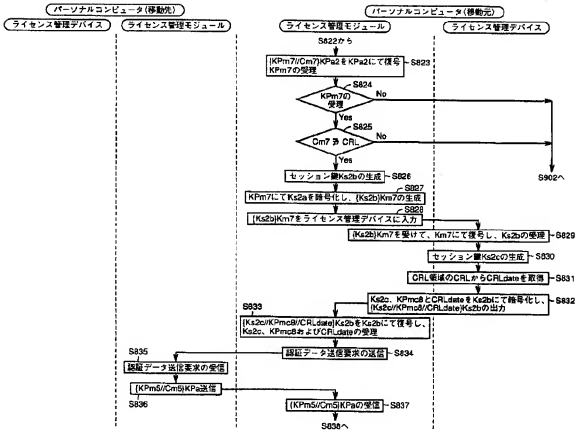
【図６８】


パーソナルコンピュータ(移動先)
ライセンス管理デバイス
ライセンス管理モジュール
ライセンス管理モジュール
開始
パーソナルコンピュータ(移動元)
ライセンス管理デバイス
レベル1ライセンス移動リクエスト
S800
ライセンス管理ファイルの暗号化機密情報を復号して
機密情報トランザクションID、コンテンツID、Ka、ACm、ACp、
チェックアウト情報およびバインディング情報)を取得
S800a
ACm再設
移動／複製可？
No
S800b
Yes
チェックアウト情報
チェックアウト済？
No
S800c
Yes
{KPm5/Cm5}KPa1をライセンス管理デバイスに入力
S801
{KPm5/Cm5}KPa1をKPa1にて復号
S802
KPm5の
受理
No
S803
Yes
Cm5 = CRL
No
S804
Yes
セッション鍵Ks2の生成
S805
S902へ
KPm5にてKs2を暗号化し、{Ks2}Km5の出力
S806
{Ks2}Km5を受けて、Km5にて復号し、Ks2の受理
S807
S808へ

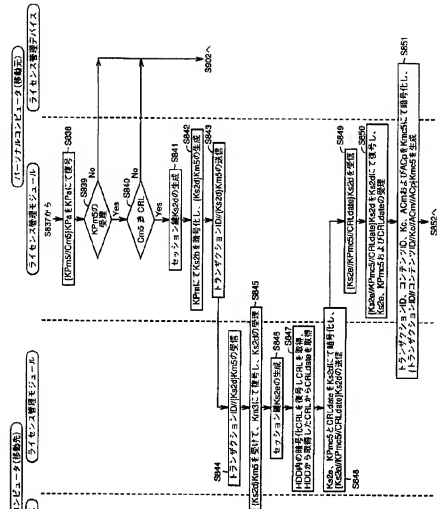
【図６９】


(パーソナルコンピュータ(携帯))
(ライセンス管理デバイス)
(ライセンス管理モジュール)
(パーソナルコンピュータ(携帯))
ライセンス管理モジュール
ライセンス管理デバイス
S807から
S808
セッション鍵Kssaの生成
S809
Kssaを[Kssa]Kssaを[Kssa]K42
をライセンス管理デバイスに入力
S810
[Kssa]Kssaを[Kssa]Kssaに復号し、Kssaを取得
S811
エントリー番号0をライセンス管理デバイスに入力
S812
エントリ番号を受領し、それに格納されている
トランザクション[Ida、コンテンツ]Ida、Kb、Acmac、およびAcpcを得る
S813
Acmacの値
No
Yes
S814
Kb、ACpcを[Kssa]Kssaに復号化し、[Kb/Acpc]Kssaを出力
S815
[Kb/Acpc]Kssaを[Kssa]Kssaに復号し、Kb/Acpcを取得
S816a
復号化確認フラグ(ACL/ICL)が立っているか
復号化確認フラグ(ACL/ICL)を参照して、
S816b
S817a
No
エントリー終了
Yes
S820
ライセンス管理デバイス入力装置データ0クリア指示
S821
[KPmt/Acmt]KPsp0/Acmを出力
S822
[KPmt/Acmt]KPsp0/Acmを受領
S823
S824
S825
S826
S827
S828
S829
S830
S831
S832
S833
S834
S835
S836
S837
S838
S839
S840
S841
S842
S843
S844
S845
S846
S847
S848
S849
S850
S851
S852
S853
S854
S855
S856
S857
S858
S859
S860
S861
S862

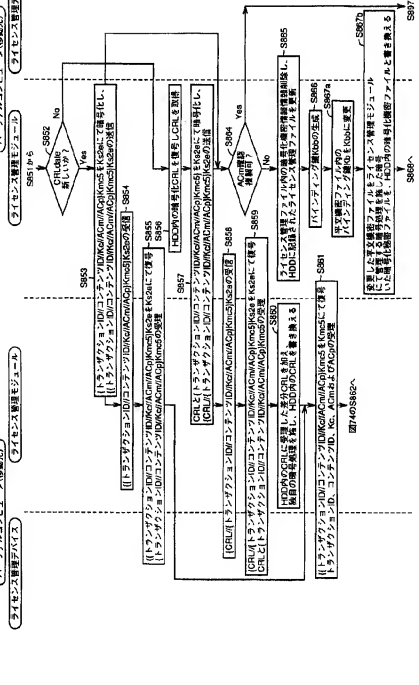
【図７０】


パーソナルコンピュータ(移動先)
ライセンス管理デバイス
ライセンス管理モジュール
パーソナルコンピュータ(移動先)
ライセンス管理モジュール
ライセンス管理デバイス
S822から
{KPm7'//Cm7}KPa2をKPa2にて復号
KPm7の受理
S823
S824
KPm7の受理
No
Yes
S825
Cm7 ∋ CRL
No
Yes
セッション鍵Ks2bの生成
S826
S902へ
S827
KPm7にてKs2aを暗号化し、{Ks2b}Km7の生成
S828
{Ks2b}Km7をライセンス管理デバイスに入力
{Ks2b}Km7を受けて、Km7にて復号し、Ks2bの受理
S829
セッション鍵Ks2cの生成
S830
CRL領域のCRLからCRLdateを取得
S831
Ks2c、KPmc8とCRLdateをKs2bにて暗号化し、
{Ks2c//KPmc8//CRLdate}Ks2bの出力
S832
S833
{Ks2c//KPmc8//CRLdate}Ks2bをKs2bにて復号し、
Ks2c、KPmc8およびCRLdateの受理
認証データ送信要求の送信
S834
S835
認証データ送信要求の受信
{KPm5//Cm5}KPa送信
S836
{KPm5//Cm5}KPaの受信
S837
S838へ

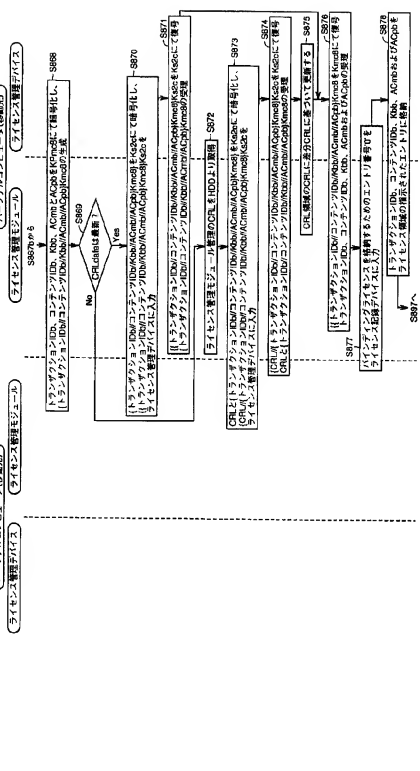
【図７１】


パーソナルコンピュータ(移動先)
ライセンス管理デバイス
ライセンス管理モジュール
パーソナルコンピュータ(移動元)
ライセンス管理モジュール
ライセンス管理デバイス
S837から
[KPrnd5/Cnt5]KPrnと[KPnd]に「0」を書き
S838
KPrnd5の
更新
S839
No
Yes
S840
Cnt5 が 0
No
Yes
セッション鍵Kcds0の生成
S841
[KPnd, FKcds1を書き込む、IKcds0]/Kmd5の生成
S842
S902へ
トランザクション0ID/[Kcds0]/Kmd5の送信
S843
S844
トランザクション0ID/[Kcds0]Kmd5の受信
S845
[Kcds0]Kmd5を受けて、Kmdに「0」を書き込む、Kcds0の作成
セッション鍵Kcds0の生成
S846
S847
HDDの領域をCRLと[CRLを 書き込む、CRLを 読み出す、CRLを 削除]
HDDの領域をCRLと[CRLを 書き込む、CRLを 読み出す、CRLを 削除]
S848
[Kcds0]/KPrnd5/CRLdata/Kcds1を作成
S849
[Kcds0/KPrnd5/CRLdata]Kcds1を送信
S850
[Kcds0/KPrnd5/CRLdata]Kcds1を受信
[Kcds0/KPrnd5/CRLdata]Kcds1と「0」を書き込む、
Kcds1, KPrnd5/CRLdata]/IDの作成
S851
トランザクション0ID, コンテンツ0ID, Kc, ACrnd1および[ACrnd1]をKmd5にて暗号化し...
トランザクション0ID/[Kcd1/Kcm1/Acpl1]Kmd5を送信
S852へ

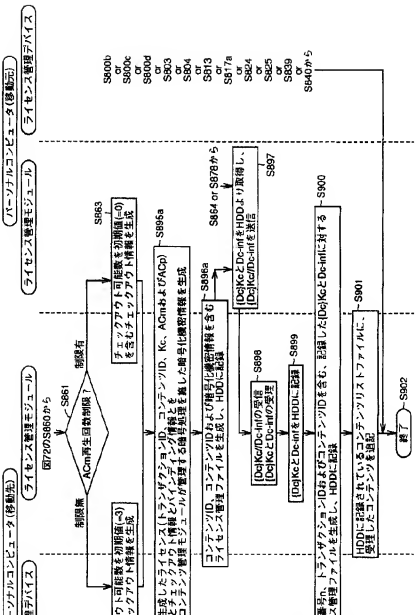
【図７２】


パーソナルコンピュータ(携帯型)
ライセンス管理デバイス
ライセンス管理モジュール
ライセンス管理サーバ(携帯型)
S851
S852
S853
S854
S855
S856
S857
S858
S859
S860
S861
S862
S863
S864
S865
S866
S867
S868
S869
S870
S871
S872
S873
S874
S875
S876
S877
S878
S879
S880
S881
S882
S883
S884
S885
S886
S887
S888
S889
S890
S891
S892
S893
S894
S895
S896
S897
Yes
No

【図７３】


パーソナルコンピュータ(携帯型)
ライセンス管理デバイス
ライセンス管理モジュール
S867からS
トランザクションIDb、コンテンツIDb、Kdb、ACmbとACpbをKmdbにて暗号化し、
トランザクションIDbのKdb/ACmb/ACpbのKmdbの生成
S868
S869
CRLのbit13 = 0 ?
No
Yes
S870
S871
S872
S873
S874
S875
S876
S877
S878
S867へ

【図７４】



フロントページの続き

(51) Int. Cl.⁷	識別記号	F I		テーマコード(参考)
		H04L 9/00	601E	
			675B	

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(71)出願人　000004167
日本コロムビア株式会社
東京都港区赤坂４丁目14番14号
(72)発明者　堀　吉宏
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(72)発明者　上村　透
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(72)発明者　畠山　卓久
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　高橋　敬幸
石川県河北郡宇ノ気町字宇野気ヌ98番地の２　株式会社ピーエフユー内
(72)発明者　常広　隆司
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所システム開発研究所横浜ラボラトリ内
(72)発明者　大森　良夫
神奈川県川崎市川崎区港町５番１号　日本コロムビア株式会社川崎工場内

Ｆターム(参考)　5J104 AA07 AA13 AA15 AA16 EA06
EA19 KA02 KA05 NA02 NA03
NA06 NA35 NA37 NA38 NA41
NA42 PA07 PA11